# **DAKOTA STATE UNIVERSITY**

# DETECTION OF VULNERABILITIES IN 5G FEMTOCELL FIRMWARE USING STATIC ANALYSIS TOOLS

A doctoral dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

October, 2023

By Charles H. Begian

**Dissertation Committee:** 

Dr. Kyle Cronin Dr. Sam Farroha Dr. Michael Ham Dr. Viki Johnson Dr. Gale Pomper



# **DISSERTATION APPROVAL FORM**

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Charles Begian Student ID: 7	7483337
--	---------

Dissertation Title:

Detection of Vulnerabilities in 5G Femtocell Firmware Using Static Analysis Tools

DocuSigned by:	
Graduate Office Verification: <i>Abby (howning</i>	Date: <u>11/06/2023</u>
F44C8D9E621C417	
	11 (00 (2022)
Dissertation Chair/Co-Chair:	Date:11/06/2023
Print Name: Kyle Cronin	
Dissertation Chair/Co-Chair:	Date:
Print Name:	
DocuSigned by:	
Committee Member: Dr. Bassam Farrolia	Date: 11/06/2023
Print Name: Dr. Bassam #216729ha4A7	
DocuSigned by:	
Committee Member: Dr. Michael Ham	Date: 11/06/2023
Print Name: Dr. Michael49#am70c7542A	
DocuSigned by:	
Committee Member: Dr. Viki Johnson	Date: <u>11/06/2023</u>
Print Name: Dr. Viki Johnson Coneque	
DocuSigned by:	
Committee Member: Dr. Gale Pomper	Date: <u>11/06/2023</u>
Print Name: Gale Pointer22DC5A41F	

Submit Form Through Docusign Only or to Office of Graduate Studies Dakota State University

#### ACKNOWLEDGMENT

My first thanks are to God, who, in His infinite mercy, has allowed this grandson of poor immigrants, from a lower-middle class family, to somehow attain a doctorate. I did not achieve this milestone solely by my own talent. Rather it was through a sequence of unexpected fortunate occurrences which I can only explain as Divine Providence. Therefore, this work is dedicated to *Deo Optimo Maximo*.

My deepest thanks go to the late Dr. Wayne Pauli. Without his encouragement, I would not have even applied for admission to DSU. Once enrolled, his constant encouragement, guidance, and "straight shooting" kept me on track, and made me a higher quality researcher. He was taken from us much too soon and is dearly missed.

I also want to extend my thanks to my very patient and long-suffering Committee. To Dr. Cronin, for taking on the unenviable job of chairing "the dissertation that refused to end", encouraging me throughout the process, and helping me overcome obstacles. Your guidance was critical to my success. To Dr. Farroha and Dr. Pomper, who volunteered to serve, despite never meeting me in person. Your commitment to helping secure our nation's 5G network speaks to who you are as professionals and serves as a model for myself and other cyber researchers. Dr. Pomper also provided the initial research idea that became my dissertation topic. To Dr. Ham, whose relentless attention to detail has greatly helped improve the quality of this dissertation. To Dr. Johnson, for reviewing the dissertation drafts from a non-technical perspective. Your comments significantly improved the readability and overall quality of the final product.

The firmware extraction was performed by Dr. Alex Otten, of the University of South Florida. Without Dr. Otten's expertise, I would not have been able to obtain my study population. Thank you, Dr. Otten, for making the execution of this study possible. Likewise, Mr. Xiaodong Zou also deserves recognition for answering my firmware extraction questions over the Internet. Your answers provided important information to support Dr. Otten's efforts.

My thanks are also extended to Mr. Earl Lum, who loaned hardware to this study to enable me to harvest an Ericsson firmware sample. Your willingness to loan that equipment to a researcher you had never met in person was greatly appreciated.

Finally, I wish to thank my wife, Lisa Begian, who never lost faith in me. Her constant encouragement ("you've got this") and support helped get me through the roughest parts of this dissertation journey. Lisa, I love you more than life itself.

#### ABSTRACT

The purpose of this study is to support fifth generation (5G) wireless network security by identifying vulnerabilities in 5G femtocell firmware. It addresses the problem of whether 5G femtocells are shipped to customers with firmware that contains vulnerabilities. This is a subproblem of supply chain security. The problem is significant because exploitation of latent vulnerabilities in the firmware of 5G network access points (such as femtocells) could compromise the security of network communications.

This study employs a design science research methodology consisting of a quasiexperiment which applies static analysis tools to 5G femtocell firmware samples. It seeks to answer the research question "can security vulnerabilities in 5G femtocell firmware be detected by static analysis tools?". The presence of vulnerabilities would imply that the firmware is insecure. This question directly supports the purpose of this research.

The quasi-experiment applied four commercially available static analysis security tools to five 5G femtocell firmware samples harvested from used 5G equipment. The static analysis tools were able to identify several known CVEs in each firmware sample. To lessen the chances of reporting false positives, each CVE reported by the tools was assigned a "confidence rating" corresponding to the number of tools reporting the presence of that CVE. The study found several CVEs in each firmware sample with confidence ratings of 1.0 (i.e., every tool in the study had reported the presence of that CVE). Further, many of these CVEs were publicly documented prior to the deployment of the firmware into the field. Because of these findings, the study was able to answer the research question in the affirmative.

# DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

\_\_\_Charles H. Begían\_\_\_

Charles H. Begian

# **TABLE OF CONTENTS**

DISSERTATION APPROVAL FORM	II
ACKNOWLEDGMENT	
ABSTRACT	
DECLARATION	V
TABLE OF CONTENTS	VI
LIST OF TABLES	IX
LIST OF FIGURES	X
CHAPTER 1: INTRODUCTION	1
BACKGROUND OF THE PROBLEM	4
STATEMENT OF THE PROBLEM	
OBJECTIVES OF THE DISSERTATION	9
SIGNIFICANCE OF THE STUDY	
NATURE OF THE STUDY	
HYPOTHESIS OF RESEARCH QUESTIONS	14
CONCEPTUAL / THEORETICAL FRAMEWORK	
DEFINITIONS / KEY TERMS	16
Assumptions	
SCOPE, LIMITATIONS, DELIMITATIONS	
CHAPTER SUMMARY	
CHAPTER 2: LITERATURE REVIEW	24
CURRENT STATE OF US DOMESTIC 5G NETWORK	24
US REGULATORY EFFORTS TO SECURE 5G	
THREAT LANDSCAPE	
CHAPTER 3: SYSTEM DESIGN (RESEARCH METHODOLOGY).	
Introduction	
RESEARCH METHODS AND DESIGN APPROPRIATENESS	
POPULATION	
SAMPLING	40
DATA COLLECTION PROCEDURES	44
VALIDITY	45
DATA ANALYSIS	47

CHAPTER SUMMARY	47
CHAPTER 4: RESULTS	49
Introduction	49
FIRMWARE PROCUREMENT	49
FIRMWARE EXTRACTION	56
SAST TOOL SELECTION AND SCAN PROCEDURE	59
FIRMWARE SCAN RESULTS	60
C1 Scan Results	60
C2 Scan Results	61
C3 Scan Results	61
C4 Scan Results	62
C5 Scan Results	62
Confidence Measurements and M <sub>1</sub> -M <sub>4</sub> metrics	63
COMMON VULNERABILITIES DETECTED ACROSS ALL FIRMWARE SAMPLES	65
FACTORS AFFECTING STUDY REPEATABILITY	68
CHAPTER SUMMARY	68
CHAPTER 5: CONCLUSIONS	69
ANALYSIS OF OBJECTIVE	69
FINDINGS	70
Determination of Truth Values for $H_0$ and $H_1$	70
Set of Reported Vulnerabilities Varies by Tool	71
Report Terminology May Increase False Positives	71
CST Sample Size Limitations	72
Each Firmware Sample Contained Multiple Vulnerabilities	72
Commercial SAST Tools Are "Works in Progress"	73
Some 5G Firmware Deployed with Known CVEs	74
Metric M <sub>1</sub> : Sample with the Highest Number of Unique CVEs	75
Metric $M_2$ : Sample with the Highest Number of Unique CVEs having $C = 1.0$	75
Metric M <sub>3</sub> : 5G Manufacturer's Firmware Most Likely to Contain CVEs	75
Metric M4: The Unique CVE Most Commonly Detected in the Sample Population	75
ASSESSMENT OF SIGNIFICANCE OF THE FINDINGS	76
Vulnerabilities are Present in 5G Femtocell Firmware, and Detectable by SAST Tools	76
Reported Vulnerabilities Vary by CST	76
Reported Information Leaks Might be False Positives	76
CST Limitations	78
5G Firmware May be Exploitable	78

Scan Results May Not be Repeatable	
Latent Vulnerabilities Exist in Fielded 5G Femtocells	
Correlation of Manufacturer to Presence of CVEs	
Significance of Metrics M <sub>1</sub> -M <sub>4</sub>	
AREAS FOR FURTHER STUDY	80
SUMMARY	81
REFERENCES	83
APPENDICES	
APPENDIX A: 454 COMMON VULNERABILITIES	
APPENDIX B: E-MAIL CORESPONDENCE	91
APPENDIX C: CST SCAN REPORT EXCERPTS FOR SAMPLE C1	94
APPENDIX D: CST SCAN REPORT EXCERPTS FOR SAMPLE C2	110
APPENDIX E: CST SCAN REPORT EXCERPTS FOR SAMPLE C3	
APPENDIX F: CST SCAN REPORT EXCERPTS FOR SAMPLE C4	
APPENDIX G: CST SCAN REPORT EXCERPTS FOR SAMPLE C5	
APPENDIX H: EFFECT OF ALGORITHM CHANGES	

# LIST OF TABLES

Table 1: Classes of 5G Wireless Access Points	2
Table 2: Commercial SAST Tools	21
Table 3: 5G devices to be tested (preliminary)	21
Table 4. 5G Network Equipment Manufacturers, in Order of Global Market Share	40
Table 5: 5G Femtocell Purchase Attempts	51
Table 6: 5G BBU boards sourced from Alibaba.com.	55
Table 7: Firmware samples, sizes, and identifiers.	60
Table 8: Number of Unique CVEs Identified in each Sample	63
Table 9: CVE findings C values	64
Table 10: Number of CVEs per sample having $C = 1.0$	65
Table 11: 454 Common CVEs by Group	67
Table 12: Ratio of CVEs Reported by Multiple CSTs / Single CST	71
Table 13: The 454 Unique CVEs Detected in Every Sample C1-C5	88

# LIST OF FIGURES

Figure 1: Non-standalone and Standalone 5G	. 25
Figure 2: 4G LTE Authentication (Dhanasekaran, 2023)	. 34
Figure 3: 5G Authentication (Dhanasekaran, 2023)	. 34
Figure 4: Sample Results Spreadsheet	. 45
Figure 5: Huawei restricts export of software	. 54
Figure 6: ZTE VSWd1 BBU controller board from Alibaba.com	. 55
Figure 7: Memory Module from Ericsson BB6648	. 56
Figure 8: Xiaodong Zou	. 56
Figure 9: ZTE VSWd1 controller board.	. 57
Figure 10: ZTE VSWc2 controller board	. 57
Figure 11: ZTE VSWd2 controller board	. 58
Figure 12: Huawei UMPTg3 with epoxied memory modules	. 58
Figure 13: Finite State Algorithm Changed to Reduce False Positives	. 74
Figure 14: Geocoordinates of ZTE VSWd2 BBU.	. 77
Figure 15: Corresponding Location of ZTE VSWd2 BBU, SW of Nanjing, China	. 77
Figure 16: CommScope Response (Sbisa, 2022)	. 91
Figure 17: Crown Castle Response (Thompson, 2022)	. 91
Figure 18: Accuver Response (Ostien, 2022)	. 91
Figure 19: FCC Clarification of Rule 22-84	. 92
Figure 20: Letter documenting FCC's quick response to inquiry on Rule 22-84	. 92
Figure 21: Offer to "white label" a Huawei BBU	. 93
Figure 22: C1 Scan Overview (Black Duck)	. 94
Figure 23: C1 Scan found 4763 Vulnerabilities (Black Duck)	. 95
Figure 24: C1 Information leaks (Black Duck)	. 95
Figure 25: C1 Asymmetric keys (Black Duck)	. 96
Figure 26: Symmetric keys (Black Duck)	. 96
Figure 27: C1 Infoleak email addresses (Black Duck)	. 96
Figure 28: C1 Infoleak IP addresses (Black Duck)	. 97
Figure 29: C1 Infoleak MAC addresses (Black Duck)	. 98

Figure 30: C1 Infoleak passwords (Black Duck)	
Figure 31: C1 Infoleak URLs (Black Duck)	
Figure 32: C1 CVEs (Black Duck)	
Figure 33: C1 Scan Overview (Code Sentry)	100
Figure 34: C1 N-day findings (Code Sentry)	100
Figure 35: C1 Vulnerabilities (mapped to CVEs in the report) (Code Sentry)	101
Figure 36: C1 Scan Overview (Jarvis)	102
Figure 37: C1 Information Leakage (Jarvis)	103
Figure 38: CVSS Severity Report (Jarvis)	103
Figure 39: CVE Summary by Severity (Jarvis)	103
Figure 40: C1 Certificates report (Jarvis)	104
Figure 41: C1 CVEs (Jarvis)	104
Figure 42: C1 email addresses (Jarvis)	104
Figure 43: C1 Password File Analysis (Jarvis)	105
Figure 44: C1 Infoleak URL report (Jarvis)	105
Figure 45; C1 Scan Overview (Finite State Platform)	106
Figure 46: C1 Scan Findings (Finite State Platform)	107
Figure 47: C1 Findings Categories (Finite State Platform)	108
Figure 48: C1 CVE Exploitability (Finite State Platform)	109
Figure 49: C2 Scan Overview (Black Duck)	110
Figure 50: C2 Scan found 4585 Vulnerabilities (Black Duck)	111
Figure 51: C2 Information leaks (Black Duck)	111
Figure 52: C2 Asymmetric keys (Black Duck)	112
Figure 53: C2 Symmetric keys (Black Duck)	112
Figure 54: C2 Infoleak email addresses (Black Duck)	113
Figure 55: C2 Infoleak IP addresses (Black Duck)	
Figure 56: C2 Infoleak MAC addresses (Black Duck)	115
Figure 57: C2 Infoleak password (Black Duck)	115
Figure 58: C2 Infoleak URLs (Black Duck)	116
Figure 59: C2 CVEs (Black Duck)	116
Figure 60: C2 Scan Overview (Code Sentry)	117

Figure 61: C2 N-day findings (Code Sentry) 118
Figure 62: C2 Vulnerabilities (mapped to CVEs in the report) (Code Sentry) 119
Figure 63: C2 Scan Overview (Jarvis)
Figure 64: C2 Information Leakage (Jarvis)
Figure 65: C2 CVSS Severity Report (Jarvis) 121
Figure 66: C2 CVE Summary by Severity (Jarvis) 121
Figure 67: C2 Certificates report (Jarvis) 122
Figure 68: C2 CVEs (Jarvis)122
Figure 69: C2 email addresses (Jarvis) 123
Figure 70: C2 URL Report (Jarvis) 123
Figure 71: C2 Scan Overview (Finite State Platform) 124
Figure 72: C2 Findings (Finite State Platform) 125
Figure 73: C2 Findings Categories (Finite State Platform) 126
Figure 74: C2 CVE Exploitability (Finite State Platform) 126
Figure 75: C3 Scan Overview (Black Duck) 127
Figure 76: C3 Scan found 4742 Vulnerabilities (Black Duck) 128
Figure 77: C3 Information leaks (Black Duck) 128
Figure 78: C3 Asymmetric keys (Black Duck) 129
Figure 79: C3 Symmetric keys (Black Duck) 129
Figure 80: C3 Infoleak email addresses (Black Duck) 129
Figure 81: Infoleak IP addresses (Black Duck) 130
Figure 82: C3 Infoleak MAC addresses (Black Duck) 130
Figure 83; C3 Infoleak passwords (Black Duck) 131
Figure 84: C3 Infoleak URLS (Black Duck) 131
Figure 85: C3 CVEs (Black Duck) 132
Figure 86: C3 Scan Overview (Code Sentry) 132
Figure 87: C3 N-day findings (Code Sentry) 133
Figure 88: C3 Vulnerabilities (mapped to CVEs in the report) (Code Sentry) 134
Figure 89: C3 Zero-day findings (Code Sentry) 135
Figure 90: C3 Scan Overview (Jarvis)
Figure 91: C3 Information Leakage (Jarvis)

Figure 92: C3 CVSS Severity Report (Jarvis)	137
Figure 93: C3 CVE Summary by Severity (Jarvis)	137
Figure 94: C3 Certificates Report (Jarvis)	137
Figure 95: C3 CVEs (Jarvis)	138
Figure 96: C3 email addresses (Jarvis)	138
Figure 97: C3 Password File Analysis (Jarvis)	138
Figure 98: C3 Infoleak URL Report (Jarvis)	139
Figure 99: C3 Scan Overview (Finite State Platform)	139
Figure 100: C3 Findings (Finite State Platform)	140
Figure 101: C3 Findings Categories (Finite State Platform)	141
Figure 102: C3 CVE Exploitability (Finite State Platform)	142
Figure 103: C4 Scan Overview (Black Duck)	143
Figure 104: C4 Scan found 2568 Vulnerabilities (Black Duck)	144
Figure 105: C4 Scan Overview (Black Duck)	144
Figure 106: C4 Asymmetric keys (Black Duck)	145
Figure 107: C4 Symmetric keys (Black Duck)	145
Figure 108: Infoleak email addresses (Black Duck)	145
Figure 109: C4 Infoleak IP addresses (Black Duck)	146
Figure 110: C4 Infoleak MAC addresses (Black Duck)	146
Figure 111: C4 Infoleak passwords (Black Duck)	147
Figure 112: C4 Infoleak URLs (Black Duck)	147
Figure 113: C4 CVEs (Black Duck)	147
Figure 114: C4 Scan Overview (Code Sentry)	148
Figure 115: C4 N-day findings (Code Sentry)	148
Figure 116: C4 Vulnerabilities (mapped to CVEs in the report) (Code Sentry)	149
Figure 117: C4 Zero-day findings (Code Sentry)	150
Figure 118: C4 Scan Overview (Jarvis)	151
Figure 119: C4 Information leakage (Jarvis)	152
Figure 120: CVSS Severity Report (Jarvis)	152
Figure 121: C4 CVE Summary by Severity (Jarvis)	152
Figure 122: C4 Certificates Report (Jarvis)	152

Figure 123: C4 CVEs (Jarvis)	. 153
Figure 124: C4 email addresses (Jarvis)	. 153
Figure 125: C4 Password File Analysis (Jarvis)	. 153
Figure 126: C4 Infoleak URL Report (Jarvis)	. 153
Figure 127: C4 Scan Overview (Finite State Platform)	. 154
Figure 128: C4 Findings (Finite State Platform)	. 155
Figure 129: C4 Findings Categories (Finite State Platform)	. 156
Figure 130: C4 CVE Exploitability (Finite State Platform)	. 157
Figure 131: C5 Scan Overview (Black Duck)	. 158
Figure 132: C5 Scan found 784 Vulnerabilities (Black Duck)	. 159
Figure 133: C5 Information leaks (Black Duck)	. 159
Figure 134: C5 Asymmetric keys (Black Duck)	. 160
Figure 135: C5 Symmetric keys (Black Duck)	. 160
Figure 136: C5 Infoleak email addresses (Black Duck)	. 160
Figure 137: C5 Infoleak IP addresses (Black Duck)	. 161
Figure 138: C5 Infoleak MAC addresses (Black Duck)	. 161
Figure 139: C5 Infoleak passwords (Black Duck)	. 162
Figure 140: C5 Infoleak URLs (Black Duck)	. 162
Figure 141: C5 CVEs (Black Duck)	. 163
Figure 142: C5 Scan Overview (Code Sentry)	. 163
Figure 143: C5 N-day findings (Code Sentry)	. 163
Figure 144: C5 Vulnerabilities (Code Sentry)	. 164
Figure 145: C5 Zero-day findings (Code Sentry)	. 164
Figure 146: C5 Scan Overview (Jarvis)	. 165
Figure 147: C5 Information leakage (Jarvis)	. 166
Figure 148: CVSS Severity Report (Jarvis)	. 166
Figure 149: C5 CVE Summary by Severity (Jarvis)	. 166
Figure 150: C5 Certificates Report (Jarvis)	. 166
Figure 151: C5 CVEs (Jarvis)	. 167
Figure 152: C5 email addresses (Jarvis)	. 167
Figure 153: C5 Password File Analysis (Jarvis)	167

Figure 154: C5 Infoleak URL Report (Jarvis)	168
Figure 155: Scan of C2 Prior to Algorithm Changes	169
Figure 156: Scan of C2 Following Algorithm Changes.	170

## **CHAPTER 1: INTRODUCTION**

From the beginning, wireless communication technologies have been insecure. Earlier wireless communication technologies included smoke signals, signal mirrors, semaphore flags, and other visual signals. Each of these technologies depended upon the human eye as the signal collector. Therefore, a physical line of sight (LOS) from the signal source to the recipient was required. A consequence of this requirement was to make the messages vulnerable to interception by any adversary who possessed an LOS to the signal source. An adversary with the means to intercept messages (and decrypt them if sent encoded) could exploit that vulnerability to eavesdrop on the communication. Modern wireless communication technologies have overcome the LOS requirement by using electromagnetic waves as their means of transmission, with a receiver device as the signal collector. Depending upon the wavelengths and modulation scheme used for transmission, signals may propagate through obstacles (such as buildings) and far beyond the line of sight (BLOS), thus overcoming a limitation of older, LOS-dependent methods (Crabtree & Kern, 2018).

The first modern wireless communication technology was radio, developed in the late 1800s. Without the application of security controls (such as encryption) to its messages, radio communication is also insecure. The omnidirectional nature of radio transmissions allows any receiver located within reception range (and tuned to the proper frequency) to receive the message. As the Imperial Russian army discovered at the battle of Tannenberg (1914) their practice of sending unencoded messages by radio (a security vulnerability) allowed their adversary to eavesdrop on their communications (exploit that vulnerability) with disastrous results for the Russians (Guthart, 2021; Jackson, 2002). The deployment of wireless communication networks which can route encrypted messages between Internet Protocol (IP) addressable devices overcomes some of the security vulnerabilities in radio communications. Encryption provides message confidentiality, digital signatures provide message integrity, and IP-based routing uses a shortest path first algorithm to minimize the number of network nodes that receive the message (thus reducing the number of possible eavesdroppers).

Like their wired counterparts, the security of wireless networks depends (in part) on the security of the devices comprising those networks. These include both end user devices which connect to the network, as well as those comprising the network infrastructure. For wireless networks, an infrastructure device that allows end user devices to connect to the network is known as a wireless access point (WAP). A wireless router that uses Wi-Fi to provide end user devices with Internet connectivity is an example of a WAP.

To access the fifth generation (5G) wireless network, the user's device first connects to a WAP. From the WAP, communications are transmitted over wired or fiber optic connections to the 5G core network. The 5G core network routes the traffic to the recipient's device, which is connected to the network over either a wired or wireless connection (i.e., connected to the network via a WAP). A listing of 5G WAP types and their numbers of supported users appears in Table 1, which is partially derived from Rodriguez' Table 3.1 (Rodriguez, 2015a).

WAP Type	Deployment Type	Number of Connections Supported
Macrocell	Cell tower	2000+
Metrocell	Urban Areas (additional capacity)	250+
Microcell	Urban Areas (coverage for localized "dead spots")	128-2568
Picocell	Large buildings, airports, train stations	64-128
Femtocell	Residential / Enterprise	4-8 (Residential) 16-32 (Enterprise)

Table 1: Classes	s of $5G$	Wireless	Access	Points
------------------	-----------	----------	--------	--------

As the connection point for user devices, 5G WAPs present an attack surface for cyber attackers. An insecure WAP potentially provides an attacker with a vector to compromise not only the WAP itself, but by extension, the 5G core network. Therefore, the cybersecurity of the aggregate 5G network depends (in part) on the cybersecurity of its WAPs. This study concentrated on the cybersecurity of indoor 5G *femtocells*, the subclass of indoor 5G WAPs which provide the fewest connections to the 5G network, as shown in Table 1. In 5G, the term "small cell" refers to several types of WAPs (metrocell, microcell, picocell, femtocell) which provide wireless access to a limited number of users in a small geographic area. A 5G femtocell is a low power wireless network access point that is designed to support a small number of users, such as in a home or small office. Femtocells are typically the smallest

capacity wireless network access points, with residential femtocells supporting 4-8 users and enterprise femtocells support 16-32 users (Rodriguez, 2015a).

WAP services are provided by the *firmware* loaded onto the WAP device by the manufacturer. The term "firmware" is used for the software resident on the WAP. It may consist of a combination of software produced by the WAP manufacturer and third-party software. Cyberattacks on WAPs via the air interface seek to leverage vulnerabilities in their firmware to compromise the targeted device. The cybersecurity of femtocell firmware is related to the number of vulnerabilities it contains, with firmware containing more vulnerabilities being viewed as being less secure. Stakeholders seeking to secure the 5G network are therefore interested in the identification of 5G WAP firmware vulnerabilities. Offensive cybersecurity researchers interested in building exploits targeting 5G WAPs are also interested, albeit from a different perspective. For them, the set of vulnerabilities identified for a specific WAP forms a group of potential pathways to compromise that device.

The purpose of this study was to determine if cyber vulnerabilities in the firmware of certain 5G wireless network femtocell devices can be detected by automated analysis tools, thereby indicating that such devices are insecure. The type of vulnerabilities detected were determined by the capabilities of the analysis tools employed but consisted of those caused by insecure coding practices, such as input buffer overflows or a lack of array bounds checking. Successful exploitation of these types of cyber vulnerabilities could allow an attacker to compromise the device. Femtocells fall into two categories: residential femtocells and enterprise femtocells. Their small size enables their deployment by end users instead of telecommunications providers. When deployed in this manner, they present a set of wireless entry points into the 5G network whose physical security and firmware configuration are managed by the device owner, instead of the network provider. This method of deployment presents security risks for femtocell users. A careless or negligent femtocell owner could introduce security vulnerabilities by misconfiguring the device or allowing extant firmware vulnerabilities to persist by not applying security patches in a timely manner. Those actions would leave the device vulnerable to malicious actors attempting to install malware. A malicious femtocell owner could purposely install malware intended to disrupt user communications or attack other parts of the 5G network. Regardless of the source of the malware installation, a compromised femtocell can be used by the attacker to eavesdrop on

the communications of legitimate femtocell users, determine their geolocation (thus violating their right to privacy) and force downloads of malware payloads to 5G devices using that femtocell for network connectivity. It could also be used for other man-in-the-middle and phishing attacks (Ahmad et al., 2019). As a network access point, a compromised femtocell could also be used to launch attacks against the 5G network itself, for example by requesting more resources from the network than it truly requires. Detection of femtocell firmware security vulnerabilities will help to protect the edge of the 5G network, as well as femtocell users.

This introductory chapter begins by introducing the 5G wireless network and describes its possible civilian and military applications. It then discusses the significance of the research in supporting 5G network security and defines the research problem. That is followed by a discussion of the research method proposed for the study, and the significance of this work to the cyber research community. The research questions to be answered are presented, along with a definition of key terms. The chapter concludes with a summary.

#### **Background of the Problem**

Wireless network security is a derivation of cyber security. Both types of security seek to ensure data confidentiality, integrity, and availability. Both may face similar classes of threats: hardware or software vulnerabilities, malicious insiders, etc. However, wireless network security must also consider the added complexity of securing multiple network access points, and the risks inherent in accepting connections with varying levels of security robustness from devices that belong to the Internet of Things (IoT). Such connections constitute threats to the wireless network infrastructure. For 5G, infrastructure threats fall into three categories: policies and standards, supply chain, and systems architecture (ESF 5G Threat Model Working Panel, 2021).

Security vulnerabilities in 5G femtocell firmware are an instance of the generalized threat of insecure 5G infrastructure. Insecure infrastructure may result from a compromised supply chain (malicious hardware or firmware deliberately installed in a network device), inadequate firmware security (device firmware containing unintentional security vulnerabilities), and misconfigured network devices (Hammi, Zeadally, & Nebhen, 2023; Morrison, 2013). Due to its role as a WAP, exploitation of a 5G femtocell's firmware

vulnerabilities could provide an attacker with a vector to further disrupt 5G network infrastructure. Malicious cyber actors have successfully attacked previous generations of wireless femtocells, resulting in a loss of communications confidentiality. For example, compromised third generation wireless (3G) femtocells have been used to clone Code Division Multiple Access (CDMA) mobile phones (DePerry, Ritter, & Rahimi, 2013).

5G is built upon previous generations of wireless network technology. First generation wireless (1G) supported analog voice transmissions and used the Advanced Mobile Phone System (AMPS) standard. Compared to contemporary mobile phones, these devices were large and heavy (e.g., the 1983 Motorola DynaTAC was a 1G device). Second generation (2G) supported digital voice, messaging, and data services, using a standard known as Global System for Mobile Communications (GSM). The 1999 Nokia 3210 is an example of a 2G device. Third generation added support for multimedia applications. Apple's 2008 iPhone 3G is an example of a 3G device. Fourth generation (4G) replaced circuit switched service with IP packet switched networking (Penttinen, 2019). It was defined by the Third Generation Partnership Project (3GPP) in Release 8 and Release 9 (3GPP, 2014a, 2014b). Current 4G service is known as 4G Long Term Evolution (4G LTE). Samsung's 2015 Galaxy S6 is an example of a 4G LTE device. 5G builds upon this foundation to offer several advantages over 4G LTE by adding support for ultra-reliable low latency communications (URLLC) massive input / massive output (MIMO) and network function virtualization (NFV). When fully deployed, 5G will support use cases for military and civilian communications, massive IoT communications, vehicle to vehicle (V2V) and vehicle to everything (V2X) among others (Bhardwaj, 2020; Penttinen, 2019; Pruitt, 2020). 5G promises to deliver 10 times higher connection density, 10 times lower latency and 100 times higher traffic capacity than existing 4G LTE networks (Pruitt, 2020).

Telecommunications operators are deploying 5G networks worldwide. While the infrastructure build required for ubiquitous 5G connectivity may require several years to achieve, the GSM Association estimates that by 2025, 50 percent of non-IoT wireless connections in the US will use 5G (GSMA Intelligence, 2020). For South Korea and Japan, the figures are 59 percent and 48 percent, respectively (Brake, 2020). The number of 5G WAPs will exceed those required for the current 4G LTE network, as the propagation characteristics of 5G radio spectra necessitate a higher density of WAPs to provide adequate

signal coverage and quality (Medin & Louie, 2019). These two factors (WAP density and number of connected devices) present malicious cyber actors with a broad attack surface. Due to the role as WAPs, 5G femtocells form part of that attack surface.

As noted previously, securing 5G femtocells presents some challenges that are not encountered when securing other types of 5G small cell WAPs. While attacks via the air interface may be attempted against any WAP, the deployment of 5G femtocells in homes and offices may provide an attacker with physical access to the device. If physical access can be obtained, then the attacker may be able to alter the femtocell's operation via an open physical interface (such as maintenance port). If the device's case can be opened, the attacker may modify the firmware (or replace the hardware with a malicious substitute). This physical attack vector is less likely to be exploited against other 5G small cell types, as they are secured by the network operator, and are mounted in locations that are not easily accessible to an attacker (such as mounted at the top of a light pole). Regardless of the attack vector used, the result is a compromised 5G femtocell, which may be used maliciously against any devices connected to that femtocell, or against the underlying 5G network itself (Osterhage, 2018). This research focuses on the detection of firmware vulnerabilities that could be exploited via the air interface, such as a buffer overflow. Detection of attacker modified firmware or hardware (i.e., from a physical attack) is outside the scope of this study.

National governments, 5G network device manufacturers, 5G network operators, public utilities, the US Department of Defense (DoD) and individual users are stakeholders in securing the 5G network. When fully deployed, the 5G network will enable a variety of use cases across several domains, such as a smart power grid, autonomous vehicles, and IoT device communications (Ericsson, 2021a). Various devices comprising the Internet of Things will also use 5G for their wireless communication technology to support their requirements for data capacity and low-latency transmission. Statista estimates that by 2025, 30.9 billion IoT devices will be deployed globally (Statista, 2016). The 5G network forms part of critical national infrastructure (CNI), and the White House has issued a national strategy for ensuring its security (Trump, 2020). In the 2020 *CISA 5G Strategy*, former CISA Director Christopher Krebs stated:

"From my perspective, 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years and, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today to secure tomorrow." (CISA, 2020)

According to Brigadier General Leleux (et. al.) securing 5G is a "whole of nation" issue, and the U.S. Government is encouraged to coordinate its efforts with industry, the DoD, and foreign coalition partners (Leleux, Woodruff, Perry, & Bergesen, 2021). DoD deems it a "critical strategic technology" (Secretary of Defense, 2020). NIST's National Cybersecurity Center of Excellence has begun development of NIST SP 1800-33 "5G Cybersecurity" (NIST, 2022) intended as a cybersecurity guide for consumers and operators of 5G network equipment. This document was in the Preliminary Draft stage at the time this study was conducted. This research endeavored to enable each of these stakeholders to improve their defenses against vulnerable 5G network equipment.

5G offers several benefits for military combat applications. For example, 5G's use of directional antennae and beamforming make transmissions harder to intercept. Unlike traditional wireless transmissions that radiate an omnidirectional signal, these technologies concentrate their signal in a narrow beam directed toward the recipient (Lumenci Team, 2021). This greatly reduces the area from which an eavesdropper could receive the transmission, as their receiver would have to be located along the transmission beam. 5G's high bandwidth and low latency support the distribution of intelligence, surveillance, and reconnaissance (ISR) data in an actionable timeframe. DoD's 5G use cases go beyond human communications to include machine to machine, and sensor to network. (Bhardwaj, 2020).

Military applications of 5G are not limited to the battlefield. 5G-enabled sensors could be used at military bases for biometric access controls or inventory monitoring (Bhardwaj, 2020). DoD is experimenting with 5G at Tyndall AFB, Florida as an enabling technology for constructing "smart bases" (AT&T, 2019). The fidelity of future military training and simulation systems (e.g., flight simulators) may benefit from 5G's low latency and high data rates.

This research is not only applicable to cyber defense. The broad potential attack surface presented by 5G offers DoD an opportunity to achieve non-kinetic effects through offensive cyber operations (OCO). The difficulties inherent in the attribution of OCO (Goel & Nussbaum, 2021) can be leveraged to support mission objectives where stealth is required (such as Special Operations missions). Once identified, cybersecurity vulnerabilities in the 5G network may be exploited to deceive an adversary, or to disrupt, deny, or degrade their 5G network capabilities, furthering DoD's capability to dominate the Cyber warfare domain. By examining 5G femtocell firmware, this research contributes to the identification of such vulnerabilities.

# **Statement of the Problem**

5G network security relies upon the cybersecurity of the underlying network infrastructure, and of the devices that connect to it. Deployed 5G network infrastructure that contains hardware or firmware security vulnerabilities presents a type of supply chain infrastructure threat. In 5G, WAPs form a heterogeneous combination of devices designed to support differing numbers of users. The 5G WAPs deployed by Mobile Network Operators (MNOs) are sourced from 5G telecommunication equipment vendors (e.g., Nokia). Therefore, the cybersecurity of each MNO's 5G network is dependent upon the cybersecurity of the WAP firmware provided by their equipment vendors. Note that the cybersecurity of this firmware is not determined exclusively by the security of the vendors' own firmware, but also by the cybersecurity of third-party firmware sourced from the vendors' supply chain.

The problem addressed by this study was to determine if 5G femtocells are shipped to customers containing firmware vulnerabilities. This is a subproblem of supply chain security. The problem is significant because exploitation of such firmware vulnerabilities could compromise the security of network communications. This research sought to answer that question by means of quasi-experimental analysis of 5G femtocell firmware. The quasi-experiment applied static analysis security tools (SAST) to the firmware of various 5G femtocell devices to identify existing cyber vulnerabilities. These tools examined the firmware instructions *statically*, that is, without executing them. This type of analysis can detect security vulnerabilities such as potential buffer overflows, unchecked array bounds, and the use of unsafe library routines. This research included the results obtained by applying a minimum of two different static analysis tools to the firmware of each 5G femtocell under study and comparing the reported cyber vulnerabilities (if any). Resource constraints limited the number of 5G femtocell firmware samples studied, with emphasis given to 5G femtocells manufactured by Huawei and ZTE, due to their designation as threats to national security (115th U.S. Congress, 2018; FCC, 2020a, 2020b).

Femtocells with firmware susceptible to comprise not only present an attacker with a vector for malicious action against devices communicating with that cell but may also present opportunities for further exploitation of the network. Previous generations of wireless femtocells (e.g. 3G femtocells) have been compromised by researchers (DePerry et al., 2013). It is precisely the security threat presented by insecure devices prompted the Federal Government to designate the networking equipment of Huawei and ZTE (both Chinese manufacturers) as a national security threat, with the FCC mandating a "rip and replace" order to telecommunication carriers (115th U.S. Congress, 2018; FCC, 2020a). Vulnerabilities identified by this research could be reported to the appropriate entity. They could also be leveraged by DoD for either defensive or offensive purposes. Used defensively, the findings may indicate which 5G network devices contain vulnerabilities and thus need firmware updates (or replacement of the femtocell with a more secure device). When used offensively, the results may provide DoD researchers opportunities to develop exploits for the compromise of an adversary's 5G network (ESF 5G Threat Model Working Panel, 2021). Telecommunications providers and consumers could also use the research results to avoid purchasing vulnerable devices.

# **Objectives of the Dissertation**

The purpose of this design science study was to support 5G network security by identifying vulnerabilities in femtocell firmware. This study employed Design Science as its research methodology. The research design consisted of examining the firmware from a set of 5G network devices. Each device's firmware was subjected to analysis by multiple SAST tools to identify vulnerabilities. The use of SAST was chosen over other experimental methods for two reasons. First, the analysis provided by the tools would likely require less time and effort than manual analysis of the firmware. Secondly, the tools provided a higher degree of code coverage than a single researcher could cover by manual analysis. The study produced artifacts consisting of scan reports of 5G femtocells produced by the tools that were used for their analysis, and the vulnerabilities identified. Where possible, identified vulnerabilities were mapped to their corresponding Common Vulnerabilities and Exposures (CVE) identifiers as maintained by MITRE Corporation (MITRE Corporation, 2021). Findings were documented for remediation by the appropriate device manufacturer or further

examination by researchers. Firmware vulnerabilities are a direct consequence of vulnerabilities in the source code (Hou, Li, & Chang, 2017). Therefore, identification of vulnerabilities requires that the firmware be subjected to some type of analysis. Design Science was an appropriate research method to study this problem because it allows development of experiments to analyze the set of instructions comprising the firmware, and their sequence of execution. Unlike qualitative studies that may provide data with differing degrees of confidence (e.g., "agree", "mostly agree"), the question of a vulnerability's existence in the firmware of given femtocell requires a binary response. That is, the vulnerability either exists in said firmware, or it does not. Further, the subject of this study (femtocell firmware) is inanimate, and therefore unable to respond to surveys such as those used in qualitative studies (Creswell & Creswell, 2017). Qualitative and mixed qualitative-quantitative methods were therefore inappropriate choices for this study's design methodology. However, both qualitative and quantitative methods were used to conduct impact analysis, enabling mitigation efforts to be prioritized.

The variables identified for this research include: the set of devices selected for study; the firmware versions tested (Have vulnerabilities in a previous firmware revision now been fixed? Has the new firmware introduced new vulnerabilities?); and the software tools used for firmware vulnerability analysis. The initial set of static analysis tools proposed for this study were the firmware tools listed by NIST (NIST, 2021), the Finite State Platform® (Finite State, 2022) Synopsys Black Duck Binary Analysis® (Synopsys, 2023) BlackBerry Jarvis® (Blackberry, 2023), and Grammatech Code Sentry® (Grammatech, 2023).

The devices included in this study were limited by project timeline and budget. The study originally anticipated that firmware samples from at least 10 devices would be examined. The device types were to include 5G femtocells from multiple manufacturers.

# Significance of the Study

The threat presented by using untrusted network devices in the 5G supply chain impacts the security of the 5G network (ESF 5G Threat Model Working Panel, 2021). The security of the 5G network is a national security issue (Trump, 2019, 2020). Cyber vulnerabilities in 5G network device firmware are a type of supply chain threat. This study sought to identify vulnerabilities in the firmware of a particular class of 5G network devices

(femtocells) to support the efforts of device manufacturers and cybersecurity researchers to improve the security of 5G network infrastructure (and by extension, support national security). Identification of such vulnerabilities allows device manufacturers to remediate them, and network operators to take mitigating actions. Remediation could take the form of issuing patches for a vulnerable device's firmware or withdrawing the device from the market. Mitigation might require network operators to apply firmware patches in the field or to remove vulnerable devices and replace them with more secure equipment.

Preliminary static vulnerability analysis of firmware has been performed by others. However, due to the relatively short time that 5G infrastructure devices have been available, they have been subjected to only limited study. The 3GPP's 5G New Radio (NR) standard was issued relatively recently, and 5G standards continue to evolve, with the latest being Release 17 (3GPP, 2023). This study differs from previous research efforts in the type of device firmware (i.e., 5G femtocell) under study. For example, Finite State took a similar approach when researching the security of Huawei 5G network device firmware, but their study concentrated on Huawei's enterprise devices and in some cases did not study the latest firmware versions for those devices (Finite State, 2019a). Huawei objected to the conclusions of the study (Huawei, 2019a) but Finite State stood by their report (Finite State, 2019b). Unlike Finite State's efforts, this research will be undertaken using current 5G devices, specifically targeting the firmware of 5G femtocells. Redini (among others) has performed static analysis of device firmware, but his study targeted IoT device firmware, not 5G femtocells (Redini, 2020).

This research supports the objectives of the *National Strategy to Secure 5G*, the *CISA 5G Strategy*, and the *Department of Defense (DoD) 5G strategy*. The DoD considers 5G to be a "critical strategic technology" (Secretary of Defense, 2020) and has recognized the strategic benefit to the United States of deploying a secure 5G network before adversaries such as Russia and China (Leleux et al., 2021). The uniqueness of this study is determined by the recency of the device firmware being examined. The 5G network is currently being deployed, and new 5G infrastructure devices are coming to market. Future IoT devices and driverless vehicles will depend on 5G communications, with the security of the underlying network affecting data privacy and vehicle safety (Osibo, Zhang, Xia, Zhao, & Jin, 2021). By examining the firmware of recent 5G devices that have not undergone extensive security

analysis, this study increased the level of knowledge about the state of 5G infrastructure security. That is of importance to 5G network device manufacturers, network operators, commercial 5G end users, and governments of nations where 5G is being deployed.

#### Nature of the Study

This research performed a design science quasi-experiment to determine if cyber vulnerabilities in 5G femtocell firmware could be detected by static analysis tools. The quasiexperiment applied static analysis tools to 5G network device firmware to discover the presence of security vulnerabilities. Where possible, the firmware samples were to be downloaded directly from the manufacturers. Otherwise, the firmware samples were extracted from physical devices by interfacing with the device hardware. That was done by reading the firmware from a programming port on the device, or failing that, de-soldering the component containing the firmware. The firmware could then be read from that component by using a chip programming device. Each firmware sample was analyzed by the same set of tools (set "S"). For each device, the results from each tool's analysis were compared to identify areas of convergence and divergence. Convergence is defined to be all tools in the experiment (all tools in set S) finding a particular vulnerability in a given firmware sample. Divergence is defined to be at least one (but not all) tools in the experiment reporting a particular vulnerability in the firmware sample. If the experimental results for a given firmware sample are convergent, there is a high probability that sample truly contains that vulnerability, and that a femtocell with that firmware is insecure. If the results are divergent, there is less confidence that the vulnerability is present in the sample (i.e., one or more tools may be reporting a false positive). It should be noted that it is possible for convergent results to be produced if all tools in S report false positive results. However, the size of set S (denoted "T") was chosen to reduce the likelihood of this occurrence to be sufficiently small so that this study's statistical power will still be at an acceptable level. The minimum value of T was computed using the G\*Power tool (Faul, Erdfelder, Buchner, & Lang, 2009), using a Type I (false positive) error rate of 5% (denoted as " $\alpha$ ") and a Type II (false negative) error rate of 10% denoted as " $\beta$ "). Creswell suggests "commonly accepted"  $\alpha$  and  $\beta$  values of 0.05 and 0.20, respectively (Creswell & Creswell, 2017), but this study attempted to achieve a lower  $\beta$ value (0.10) and a statistical power  $\geq 0.90$ . In instances where no tool in the experiment

reported the presence of a vulnerability for a given sample, the firmware still cannot be assumed to be free of that vulnerability with 100% confidence, as the possibility exists that the entire set of tools could be reporting false negative results. The value of  $\beta$  was chosen to limit the possibility of that occurrence. A discussion of the power analysis values used to determine the sample size is provided in Chapter 3.

The analysis results for each firmware sample were then summarized by comparing the number of tools reporting a given vulnerability (*V*) to the number of tools (*T*) in set *S*. The confidence (*C*) that a firmware sample contains a reported vulnerability is given by the formula below. Note that the probability of all tools reporting a false negative ( $\epsilon$ ) is small but not zero ( $0 < \epsilon < (\frac{1}{r})$ ) and decreases as *T* increases.

$$C = \begin{cases} V/T & if \ V \ge 1\\ \epsilon & if \ V = 0 \end{cases}$$

The subject population of this study was the set of firmware samples themselves. The results are a set of a numeric confidence ratings (each sample will have one instance of C per identified vulnerability). The tools in set S are the values of the experiment's independent variable, with C being a dependent variable. The nature of the research question (a closed question) and the binary nature of the experimental results (firmware sample X [contains | does not contain] vulnerability Y) resulted in the use of Design Science methodology for the experiment (Wieringa, 2014).

The use of a design science methodology was chosen over quantitative, qualitative, or mixed quantitative/qualitative approaches, as this research does not involve human subjects, nor do its experiments produce results with a subjective range of values (experimental results are *not* of the form: firmware sample X "always | usually | sometimes contains" vulnerability Y). For those reasons, neither a qualitative nor mixed method approach is suitable.

This research sought to answer the question: can cyber vulnerabilities in 5G femtocell firmware be detected by static analysis tools? It intended to examine this question by repeating its experiment on the firmware of 5G devices from several manufacturers. Vulnerabilities thus identified were used to answer the research question.

# **Hypothesis of Research Questions**

This study sought to answer only a single central research question and one subquestion. The central research question was "can security vulnerabilities in 5G femtocell firmware be detected by static analysis tools?". The presence of vulnerabilities would imply that the firmware is insecure. This question directly supports the purpose of this research. If vulnerabilities are found, the implication is that the associated 5G femtocells are insecure, enabling manufacturers to take steps to remediate the vulnerabilities, thereby contributing to the solution of the research problem of 5G device supply chain security. The sub-question posited that if a 5G femtocell firmware sample contains a vulnerability, at least one of the analysis tools in set *S* would detect it. To improve the accuracy of the research, the tools comprising *S* were chosen with emphasis on selecting those which have been recognized by industry or used in peer-reviewed research.

Two hypotheses flow from these research questions, both of which were tested in this study. First, the null hypotheses ( $H_0$ ), which states that there are no detectable vulnerabilities in the 5G femtocell firmware samples. This hypothesis could be supported by having all the tools in *S* fail to find vulnerabilities in any of the firmware samples. While this would be a necessary condition for  $H_0$ , it would not be a sufficient condition. Note that if the results of this study had supported  $H_0$ , the answer to the research sub-question would be indeterminant. The second hypothesis ( $H_1$ ) states that a significant amount of 5G femtocell firmware contains vulnerabilities and is therefore exploitable. That is, multiple firmware samples in the population studied will have at least one vulnerability. Based on the Finite State's previous work on Huawei enterprise 5G firmware (Finite State, 2019a) and Redini's work on IoT firmware (Redini, 2020) this research was anticipated to satisfy the postulation of  $H_1$  (at least for Huawei products). As such,  $H_1$  can be classified as a *directional hypothesis*, because it anticipates the research results (Creswell & Creswell, 2017). Further note that verification of  $H_1$  is sufficient to affirmatively answer the research sub-question.

#### **Conceptual / Theoretical Framework**

In quantitative research, *independent* variables determine the research outcomes. Variables modeling those outcomes are known as *dependent* variables (Creswell & Creswell, 2017). This study utilized one independent and one dependent variable. These were:

*X*: (independent variable) 5*G* femtocell firmware's manufacturer (e.g. Huawei)

*Y*: (dependent variable) sample contains at least one vulnerability (is insecure)

Each firmware sample has an associated manufacturer. The manufacturer's internal firmware development practices (such as enforcement of secure coding) can reduce firmware vulnerabilities, such as those noted by Yao and Zimmer (Yao & Zimmer, 2020). This research sought to find a correlation between the firmware sample manufacturer (*X*) and the presence of vulnerabilities in their firmware samples (*Y*). A correlation found for certain manufacturers (e.g., X = Huawei) but not for others (e.g., X = Nokia) may imply that device manufacturer  $\rightarrow$   $H_1$ . If no vulnerabilities are found in any of the firmware samples,  $H_0$  is implied (and  $H_1$  disproven). The expected outcomes of this study were that  $H_1$  will be found to be true (at least for X = Huawei, and possibly for other manufacturers), and  $H_0$  found to be false.

These outcomes are projected by generalizing previous research by Finite State, Inc. (Finite State, 2019a) and the United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board (HCSEC, 2019). Finite State examined almost 10,000 firmware samples from over 500 Huawei enterprise networking products. They found several known vulnerabilities in the Huawei products, with over 1400 vulnerabilities being found in the firmware of a single device. Finite State traced many of these vulnerabilities to Huawei's use of third-party and open-source libraries. Other reported vulnerabilities were functions that were susceptible to buffer overflow attacks, and possible backdoor access. Over 60 firmware samples contained host key files (Finite State, 2019a). Huawei disputed the contents of the report, stating that "None of the Huawei products tested by Finite State will be deployed for 5G RAN or Core in telecommunications networks." Huawei also raised other objections to the report, claiming that Finite State had not tested the latest versions of their software (implying that Huawei may have already patched the reported vulnerabilities) and complained that Finite State had not given Huawei an opportunity to review the report findings prior to publication (Huawei, 2019a; Huawei PSIRT, 2019b). This drama continued with Finite State issuing a reply to Huawei's response to Finite State's report. The reply reiterated the report's

assertion that Huawei's firmware security had worsened over time and accused Huawei of engaging in ad hominem attacks against Finite State. For example, according to that reply, Huawei accused Finite State of lacking "maturity and competence" and that "Huawei would be happy to teach Finite State the basics of imbedded [*sic*] systems and global telecommunications operations that cover the globe" (Finite State, 2019b; Huawei PSIRT, 2019b).

Since 2014, the United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board (UK HCSEC) has sought to mitigate the potential cyber risk arising from the use of Huawei products in the UK's critical infrastructure. The HCSEC "provides security evaluation for a range of products used in the UK telecommunications market" (HCSEC, 2019). Its 2019 annual report (dated March 2019) raised concerns about Huawei's software development practices, expressed concern about the security risks posed by Huawei equipment already in use in the UK, and noted the lack of progress made by Huawei in addressing the defects listed in the previous year's (2018) HCSEC report (HCSEC, 2019).

The above-cited research indicates that Huawei's networking products have firmware vulnerabilities and exposes Huawei's sensitivity to having them publicly reported. The HCSEC report also indicates that Huawei's software development practices do not ensure secure firmware, and that Huawei is slow to remediate vulnerabilities that are reported. Given these observations, this research anticipated that Huawei's 5G femtocell firmware would suffer from the same type of unpatched security vulnerabilities reported for its enterprise network equipment, and that such vulnerabilities would be revealed by static analysis tools. Therefore, it predicted that for Huawei  $H_1$  will be proven, and  $H_0$  disproven. No prediction is made for the provability of  $H_1$  and  $H_0$  for other manufacturers included in this study.

## **Definitions / Key Terms**

*1G:* First Generation wireless network. Limited to analog voice communications (Penttinen, 2019).

2G: Second Generation wireless network. Digital voice, messaging, and data services (Penttinen, 2019).

*3G:* Third Generation wireless network. Digital voice, messaging, data, and multimedia support (Penttinen, 2019).

*3GPP:* Third Generation Partnership Project. A group of organizations which define standards for wireless communications (Penttinen, 2019).

*4G:* Fourth Generation wireless network. Offers digital communications of 3G, but replaces circuit switched service with IP packet switched networking (Penttinen, 2019).

*4G LTE:* Fourth Generation wireless network with Long Term Evolution. An implementation of 4G specified in the 3GPP Release 8 specification. Sometimes referred to as "3.9G" (Penttinen, 2019).

5G: Fifth Generation wireless network. Expands the capabilities of 4G by adding support for ultra-reliable low latency communications, massive input / massive output WAPs, and increased data rates. Defined in 3GPP Release 16 specification (3GPP, 2021).

*5G Core:* Core functionality of 5G backhaul network. Defined in 3GPP Release 16 specification (3GPP, 2021).

*5G RAN:* 5G fronthaul Radio Access Network (RAN). Defined in 3GPP Release 16 specification (3GPP, 2021).

*CDMA:* Code Division Multiple Access. A radio network used by MNOs to allow calls and data from multiple users to share a radio channel. CDMA encodes each call's data with a unique key. Then all calls are transmitted at once, with receivers "dividing" the combined signal back into individual calls (Verizon, 2020).

*CNI:* Critical National Infrastructure. "There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (CISA, 2020b).

*Convergence:* Occurs when *all* tools in the experiment (that is, all tools in set *S*) find a particular vulnerability in the same firmware sample.

Dependent variable: In quantitative research "dependent variables are those that depend on the independent variables; they are the outcomes or results of the influence of the independent variables" (Creswell & Creswell, 2017).

*Directional Hypothesis:* A hypothesis where "the investigator makes a prediction about the expected outcome, basing this prediction on prior literature and studies on the topic that suggest a potential outcome" (Creswell & Creswell, 2017).

*Divergence:* Occurs when at least one (*but not all*) tools in the set *S* report a particular vulnerability in a particular firmware sample.

*Femtocell:* The smallest capacity WAPs. Residential femtocells typically support 4-8 users, while enterprise femtocells support 16-32 users (Rodriguez, 2015a).

*Firmware:* The lowest layer of software, functioning between the operating system or hypervisor layer and the hardware itself (Yao & Zimmer, 2020).

*Independent variable*: In quantitative research, "*independent* variables are those that influence, or affect outcomes in experimental studies" (Creswell & Creswell, 2017).

*MIMO*: Multiple Input / Multiple Output. A technique for providing increased data transmission rates by using multiple antennae concurrently. Due to the benefits offered by antenna beamforming in 5G, this is sometimes called "massive MIMO" (Stepanets, Fokin, & Müller, 2019).

*NFV:* Network Function Virtualization. Network functions are performed virtual devices (i.e. software) instead of by dedicated hardware. NFV is "a principle of separating network functions from the hardware they run on by using virtual hardware abstraction" (Penttinen, 2019).

*Pseudo-stratification:* The practice of selecting a sample of research subjects whose characteristics may not be representative of the population. This is in contrast to stratified sampling, which selects samples that represent the characteristics under study in proportion to their occurrence in the population.

*Quasi-experiment:* A research design method where the "assignment of a treatment to objects of study is not random. This means that the sample is not selected randomly from the population, and/or treatments are not allocated randomly to elements of the sample" .(Wieringa, 2014)

*Reproducibility:* "The measurement can be obtained with stated precision by a different team using the same measurement procedure, the same measuring system, under the same operating conditions, in the same or a different location on multiple trials. For computational experiments, this means that an independent group can obtain the same result using the author's own artifacts" (ACM, 2020).

*Replicability:* "The measurement can be obtained with stated precision by a different team, a different measuring system, in a different location on multiple trials. For

computational experiments, this means that an independent group can obtain the same result using artifacts which they develop completely independently" (ACM, 2020).

*Static Analysis Security Tool (SAST):* An automated tool that can scan software/firmware to identify vulnerabilities. Certain SAST tools operate only on source code, while others can scan binary object code as well.

*URLLC*: Ultra Reliable Low Latency Communications is a "new service category in 5G to accommodate emerging services and applications having stringent latency and reliability requirements" (Ji et al., 2017).

*WAP*: Wireless network access point. A network node which permits users to connect to the network via a radio interface.

#### Assumptions

The success of this research depended upon the following assumptions. First, that the requisite number and type of static analysis tools would be available. The G\*Power tool indicated that 13 samples are required to meet the minimally acceptable  $\beta$  of 0.2 and statistical power of 0.80 suggested by Creswell (Creswell & Creswell, 2017). At least 16 samples are required to achieve a more desirable statistical power of 0.90. The availability of 5G femtocell firmware samples was also assumed. The United States was currently experiencing supply chain issues due to the global Covid-19 pandemic, and the ready availability of Chineseproduced (Huawei and ZTE) products was not assured. Second, it was assumed that the firmware of the femtocells under study could be extracted for analysis or downloaded from the manufacturer's website. The study also recognized the possibility that the devices might have security controls which inhibit the exfiltration of their firmware, and the firmware may not be available for download. Should both situations have occurred for certain 5G femtocells, other 5G femtocell devices will be substituted. Third, the analysis tools selected for set S must be able to analyze the firmware. If they had been incompatible with the firmware, other analysis tools would have been substituted. Finally, the analysis tools selected for inclusion in set S must report accurate results. That is, they must not report any false negative or false positive results. The list of firmware analysis tools specified by NIST (NIST, 2021) and commercial Static Analysis Security Tools (SAST) were anticipated to satisfy this condition.

#### Scope, Limitations, Delimitations

The scope of this study consisted of firmware samples from the top global manufacturers of 5G femtocell devices. These devices were selected as representative of their 5G femtocell product lines. Firmware from Huawei and ZTE devices was given preference for study over firmware from other manufacturers. That was because previous research has shown that Huawei 5G products contained vulnerabilities (Finite State, 2019a; HCSEC, 2019) and both ZTE and Huawei have been designated as national security threats (115th U.S. Congress, 2018; FCC, 2020a). The scope of this study excluded femtocells from wireless networking generations other than 5G. The reasons for restricting the scope to 5G was due to the criticality of 5G security to DoD and the Nation (Leleux et al., 2021; Trump, 2020). This research only examined indoor 5G *femtocell* firmware. Firmware from other types of 5G small cells (micro cell, picocell, etc.) was outside the scope. By identifying vulnerabilities in 5G femtocell firmware, a topic not yet extensively studied in scholarly literature, this study aimed to expand the body of knowledge in the offensive cyber research community.

Terrel states that "Limitations are constraints outside of the control of the researcher and inherent to the actual study that could affect the generalizability of the results" (Terrell, 2015). This research was limited by the type of devices selected for study (5G femtocells), the size of the set of devices studied, and the decision to restrict the firmware samples to those from those with larger worldwide 5G market share. Each of these factors was impacted by the availability of resources (time and budget). The decision to limit the study to 5G femtocells (instead of multiple types of 5G small cells) was driven by budget considerations. The generalizability of the results of this research on 5G femtocell devices from other manufacturers is yet to be determined. The decision to limit the number of studied firmware samples was driven by time and budget constraints. It was impossible to include all 5G femtocell firmware in this study within the time and budget available to the researcher. Even if sufficient time and budget had been available, certain manufacturers' devices might be unobtainable, due to import restrictions, supply chain problems, or excessive demand. The possibility exists that while the size of the population of firmware samples selected for this research may limit the generalizability of the study, it still may, at the very least, provide a foundation for the work of future researchers. This study was limited to testing products from the five manufacturers having the largest share of the global 5G networking market, as

research budget limitations make it impractical to test samples from every possible manufacturer. This impacted the generalization of the results to the 5G femtocells of other manufacturers, but it also presents an opportunity for future research. Due to the threat presented to national security (115th U.S. Congress, 2018), Huawei and ZTE 5G femtocells were given precedence in selection of the research sample. However, they were difficult to obtain, due to the FCC ban on the use of their products in US networks (FCC, 2023). Should they prove to be unobtainable, the study had planned to compensate for their absence by increasing the representation of other manufacturers' 5G femtocells in the sample. The selection of 5G femtocells available for this study was anticipated to be constrained by the supply chain issues caused by the Covid-19 pandemic. As a result, firmware samples from other 5G femtocell devices were to have been to be substituted for some of the planned research population. This had a negative effect on the generalization of the research results. The set of commercial SAST tools to be included in set *S* is limited by the availability of such tools to the researcher. A preliminary list of commercial SAST tools to be used is given in Table 2, and a preliminary list of 5G femtocell devices to be tested is provided in Table 3.

Table 2: Co	ommercial	SAST	Tools
-------------	-----------	------	-------

Commercial SAST Tool	Version
Blackberry Jarvis®	2.0
Finite State Platform®	August 2023
Grammatech Code Sentry®	5.0.0
Synopsys Black Duck Binary Analysis®	2023.7.0

Table 3: 5G devices to be tested (preliminary)

Manufacturer	Device
Ericsson	BB6648
ZTE	VSWc2
ZTE	VSWd1 NVMe
ZTE	VSWd1 eUSB
ZTE	VSWd2

Terrel defines delimitations as "further limitations actively put into place by the researcher in order to control for factors that might affect the results, or to focus more specifically on a problem" (Terrell, 2015). This research was also limited by the capabilities of the set of firmware analysis tools (set *S*) used to evaluate the firmware samples. It was possible that one or more firmware samples could contain vulnerabilities which escaped detection by each tool (every tool gives a false negative result). While the probability of this occurrence was believed to decline as the size of *S* was increased, it could not be reduced to zero. Therefore, it should be noted that firmware samples evaluated to contain no vulnerabilities might contain one or more vulnerabilities which are undetectable by the set of tools selected for this research. This research is further delimited by only considering firmware vulnerabilities that may be exploited via a femtocell's air interface. The presence of vulnerabilities introduced by malicious actors having physical access to the device was not studied.

Removed of those constraints, this research could be extended for by examining different 5G devices than those contained in this study, by using different static analysis tools, by adding dynamic analysis of firmware behavior, or by performing analysis on open-source 5G software, such as O-RAN.

# **Chapter Summary**

This chapter introduced the topic of this study. It described the project background, relating the research to the broader topic of wireless network security. It classified insecure 5G femtocell firmware as an instance of a supply chain type of 5G infrastructure threat. It briefly summarized the evolution of wireless communications from 1G to 5G. It discussed the projected effect of the deployment of 5G, for both civilian and military users. It presented the topic's importance to the cybersecurity research community and to national security. The applicability of this research to offensive cyber operations is also noted.

The problem and plan for the associated research was presented. A problem statement was defined, showing the relationship between the larger problem of wireless network security, the threat posed by insecure WAPs connected to the 5G network, and 5G femtocells containing insecure firmware. That was followed by the study's purpose statement that relates its goals to the broader objective of ensuring 5G network security. The design methodology

and research question were introduced. The importance of this study, and its significance among related research in the field, was described.

The nature of the design science research quasi-experiment was presented, describing the research methodology used to design the experiment, its parameters, research variables, and the criteria used to evaluate the results. The research questions to be answered are noted, along with a null hypothesis and a directional hypothesis. The theoretical framework of the study was discussed and compared with similar studies in the research area. That was followed by a list of pertinent terms and their definitions. The research assumptions and their rationale were described, with mitigation plans for assumptions that might prove to be incorrect. The chapter concluded by describing the scope, limitations and delimitations underlying this research.

Chapter 2 will present a review of the pertinent literature reviewed for this study. It covers topic areas such as the current state of the US domestic 5G network, efforts by the US Government to secure 5G, the threat presented by insecure 5G WAPs, firmware vulnerability analysis, and previous vulnerability analysis of other Huawei and IoT devices.

# **CHAPTER 2: LITERATURE REVIEW**

This chapter surveys the recent literature pertinent to the topic of this study. We begin laying a foundation by describing the current state of the 5G network in the United States (Summer, 2023). Then we will discuss US Government and DoD efforts to secure the domestic and military 5G networks. This is followed by a summary of 5G network security architecture. This chapter concludes with a discussion of related research in wireless network device security vulnerabilities, with emphasis on those pertaining to 5G network device firmware.

#### **Current State of US Domestic 5G Network**

In the US, AT&T, Verizon, and the recently merged Sprint/T-Mobile USA are each building out their domestic 5G networks (Pruitt, 2020). Deployment of the commercial 5G network is coordinated by the National Economic Council (NEC) (GAO, 2020b). In this initial phase of 5G deployment, the service being fielded is known as "non-standalone" (NSA) mode. NSA mode uses a 5G radio access network (RAN) coupled with a 4G evolved packet core (EPC) network on the back end. One characteristic of this design is that all control plane (network control and administration) traffic is routed through the 4G network (LTE radio interface and EPC). While user equipment (UE) connects to an NSA 5G network over a 5G RAN, only user plane data (user communications) flow over the 5G radio interface. Control plane functions (such as network authentication) are still supplied to the UE over the 4G LTE radio interface. As 5G infrastructure build-out continues, the 4G EPC will be replaced by the 5G core network (5GC). When the 5G RAN is used with the 5GC, the resulting network is said to be in "standalone" (SA) mode. In SA mode, the UE does not connect to the 4G LTE RAN. Rather, it connects to the 5G RAN for service of both user plane and control plane communications (Figure 1).

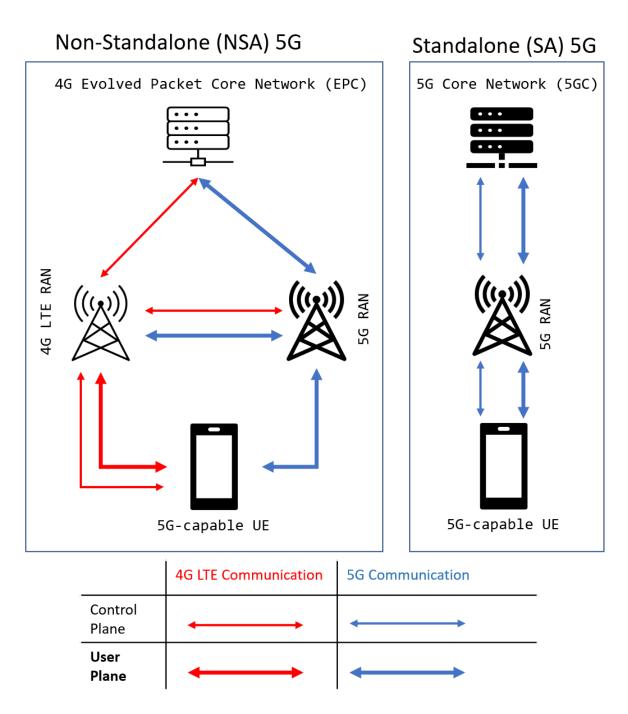


Figure 1: Non-standalone and Standalone 5G

Domestic carriers have selected two primary frequency bands for 5G deployment. The first consists of sections of the 2.5GHz-6.0GHz band (at 2.5GHz, 3.5GHz, and 3.7GHz). These frequency ranges are known as the "mid" or "sub-6" bands. The second consists of frequencies above 24.0Ghz, known as the "millimeter wave" (mmWave) band (GAO, 2020a) . In addition to these primary bands, T-Mobile USA offers a "low-band" (600MHz) 5G

service targeted at rural areas (T-Mobile USA, 2020) while AT&T's low-band service operates at 850MHz. Although these low-band deployments are unable to support 5G's high data rates, they are used to provide adequate signal coverage over sparsely populated (i.e., rural) areas.

Selection of RF spectra presents 5G carriers with a trade-off between coverage and available bandwidth. The RF transmissibility characteristics of the mid-band spectra differ from those of mmWave. The sub-6 band offers better signal propagation than mmWave. Its longer wavelength provides better obstacle penetration than mmWave (the latter can be blocked by walls or trees). Conversely, by virtue of its shorter wavelength, mmWave signals form a narrower beam than sub-6 transmissions, making them more difficult to intercept. The longer range of the sub-6 band (as compared to mmWave) allows sub-6 base stations to be deployed more sparsely than mmWave base stations, thereby lowering the deployment cost of providing coverage to a given geographic area. To realize the high data transfer rates promised by 5G, up to five contiguous 100MHz channels can be combined. In the US, adequate contiguous spectrum exists in the mmWave band (especially above 28.0GHz) to support these 500MHz channels. However, among those nations deploying 5G, the US faces a unique challenge. The domestic sub-6 band is fragmented between several current users, making it difficult to assign carriers large amounts of contiguous bandwidth. Much of the sub-6 band is owned by the US Government and is in active use. Although migration of some current users to other frequency bands is possible, it will take considerable time and investment to achieve (Medin & Louie, 2019).

Sub-6 band user migration is further complicated by an administrative division within the US Government. The Communications Act of 1934 (47 USC) specifies that the Federal Communications Commission (FCC) manages non-Federal users of the RF spectrum, while the National Telecommunications and Information Administration (NTIA) performs the same role for Federal users. The NTIA's strategy is given in their National Spectrum Strategy, while the FCC's is described in the Facilitate America's Superiority in 5G Technology Plan (GAO, 2020b). Note that these two arms of government manage sets of RF spectrum users, and not ranges of the spectrum itself. Thus, moving Federal users from parts of the sub-6 spectrum to free those frequency ranges for use by non-Federal 5G users necessarily requires coordination of both the NTIA and FCC (Nebbia, 2010). Domestic carriers are deploying 5G on a mix of sub-6 and mmWave bands. For example, T-Mobile USA is deploying 5G on mmWave in densely populated urban areas and on sub-6 bands in suburban areas. It is also deploying on the 600MHz band in rural areas, benefiting from the better propagation of the longer wavelength signal (but at a sacrifice in data rate). AT&T is also deploying 5G across mmWave, sub-6 and low-band (850MHz) frequencies. Verizon has no low band offering, instead deploying broadband 5G on the mmWave (28.0GHz) band (Pruitt, 2020).

The DoD and domestic 5G providers face interoperability challenges with the global 5G network. For example, while the sub-6 band is desirable for 5G communications (due to its signal propagation characteristics), its availability in the US is limited due to competing uses. Thus, mmWave band network and user equipment will dominate the US 5G network. However, several nations are actively deploying 5G network services. Outside the US, the sub-6 spectrum is not similarly constrained, so sub-6 band 5G network infrastructure and UE will prevail there. This limits the usefulness of 5G network equipment designed for the US market. Likewise, such equipment designed for the foreign market may not operate in the US. This has supply chain implications, as the domestic 5G market is smaller than the non-US market, limiting the choice of vendors for domestic 5G network infrastructure. These differences also pose a challenge for DoD as their missions are primarily conducted outside the US, where they could be required to use host nation 5G infrastructure, which may not be interoperable with their systems (Pruitt, 2020).

## **US Regulatory Efforts to Secure 5G**

The Federal Government has undertaken several steps to secure the nation's cyber infrastructure, including the domestic 5G network. President Trump approved the *National Cyber Strategy* in September 2018 (Trump, 2018), designating that the Department of Homeland Security (DHS) is responsible for securing Federal department and agency networks. National security systems or intelligence community networks remain secured by the National Security Telecommunications and Information Systems Security Committee under National Security Directive 42 (United States White House Office, 1990). The *National Cyber Strategy* identified 5G as a target for malicious cyber actors, advocating that the Federal Government work with the private sector to secure information and communications technology (ICT), viewing ICT providers as cyber enablers.

On May 15, 2019, Trump issued Executive Order (E.O.) 13873, which declared a national emergency regarding the exploitation of ICT vulnerabilities by foreign adversaries:

"I further find that the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." (Trump, 2019)

There are five major vendors of 5G core network hardware in the global marketplace (Brake, 2020; Finite State, 2019a). None of them are headquartered in the United States. Two of the five having the largest share of the global market, Huawei and ZTE, are Chinese firms. The others are Nokia (base in Finland), Ericsson (Sweden) and Samsung (South Korea). Huawei alone controls 29 percent of the global telecommunications market (Center for a New American Security, 2020). Executive Order 13873 excludes the two largest 5G equipment suppliers from the US market (Trump, 2019). While the security concerns raised in E.O. 13783 give compelling reasons to do so, a side effect of that action is to limit competition in the US market, which may increase the cost of domestic deployment of 5G network infrastructure. Limited competition also exists in the manufacture of commercial 5G New Radio (NR) devices, where Qualcomm is the only domestic supplier (Pruitt, 2020).

Twelve days prior to the release of E.O. 13783 (i.e., May 3, 2019) the Prague 5G Security Conference issued a set of proposals (*"The Prague Proposals"*) for securing the global 5G network. This conference included representatives from 32 countries, including the United States (GAO, 2020b). The proposals included an affirmation of the rights of each participant nation to "set their own national security and law enforcement requirements" while maintaining compliance with international law. The proposals also recommended that vulnerability assessments and risk mitigation be performed for all "components and network systems" (Prague 5G Security Conference, 2019).

The 116<sup>th</sup> Congress passed the Secure 5G and Beyond Act of 2020, which was signed into law on March 23, 2020. This law mandated that the President develop a strategy to secure next generation wireless systems and infrastructure (GAO, 2020b). It further required the development of an implementation plan for that strategy. Both the strategy and associated implementation plan were to be delivered to Congress within 180 days of the law being adopted. The law also prohibited the strategy from advocating the nationalization of the domestic 5G network or any future wireless networks (120th U.S. Congress, 2020).

Elements of *The Prague Proposals* and *National Cyber Strategy* were incorporated into the *National Strategy to Secure 5G* (released on March 23, 2020 – the same day PL 116-129 was adopted). This document emphasized deployment of the domestic 5G network, assessment of risks and security principles in the 5GC, and management of the economic and national security risks resulting from use of 5G. It recognized that the 5G network would likely be a target of cyber criminals and foreign adversaries for financial gain and intelligence collection (Trump, 2020).

NTIA released the corresponding implementation plan on behalf of the President on January 6, 2021. The *National Strategy to Secure 5G Implementation Plan* expanded on the four "lines of effort" listed in the *National Strategy to Secure 5G*. It emphasized the importance of supply chain security to ensuring security of 5G infrastructure. It also highlighted the importance of assessing risks to national security (and to the US economy) that may result from the global deployment of 5G and called for the Government to encourage industry to mitigate known 5G security vulnerabilities by using a combination of incentives and policy decisions. It recognized the importance of international standards to ensuring the security of the global 5G network and advocated that the US play a leadership role in creating those standards (NTIA, 2021). However, given the closure of the US market to major 5G network device manufacturers (Huawei, ZTE) and the foreign vs. domestic 5G interoperability issues mentioned above, the US may find that its ability to influence global 5G standards is limited. Development of domestic 5G standards is overseen by the 3GPP (Pruitt, 2020).

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is responsible for the cybersecurity of the US critical national infrastructure (CNI). CISA collaborates with 5G standards bodies, working groups, and national laboratories to discover security vulnerabilities in 5G network components. The agency released its *CISA 5G Strategy* on August 24, 2020. That document recognized that 5G infrastructure will present a broad attack surface for malicious cyber actors. CISA proposes to mitigate that threat by working in conjunction with national laboratories and academia to test 5G network equipment and identify vulnerabilities. CISA also proposes to collaborate with other Federal agencies in 5G research and development (R&D) activities such as Open RAN (CISA, 2020). Their support of open 5G standards (e.g. Open RAN) is in agreement with DoD's advocacy of the same through the Office of the Undersecretary of Defense (Stacey, 2019).

The Department of Defense has recognized 5G as a "critical strategic technology" (Secretary of Defense, 2020) and is evaluating it for applicability to their missions. DoD is testing five use cases for 5G technology Augmented/Virtual Reality, Smart Warehousing (transshipment), Smart Warehousing (vehicle storage and maintenance), Distributed Command and Control, and Dynamic Spectrum Utilization as described in (DoD, 2020a). These test sites realize one of the Defense Science Board's recommended 5G strategy actions (Defense Science Board, 2019). On May 2, 2020, DoD released the Department of Defense (DoD) 5G Strategy. The strategy states that DoD requires "resilient and protected 5G capabilities and spectrum" and commits DoD to supporting the furthering of US and partner nation 5G capabilities. DoD's interest in 5G spectra includes both sub-6 and mmWave bands. Defensively, DoD is to support the development of technologies to protect 5G infrastructure and identify national security risks resulting from 5G. The identification of security vulnerabilities and possible mitigation strategies is a consistent concern (Defense Science Board, 2019; Secretary of Defense, 2020; Trump, 2020). DoD also seeks to cooperate with industry, Federal agencies, Congress, and partner nations to mitigate 5G security vulnerabilities. Of these, industry is viewed as being the only partner who can satisfy DoD's 5G requirements, due to the commercial sector's greater 5G R&D resources (Secretary of Defense, 2020).

The strategy was followed by the release of the *Department of Defense 5G Strategy Implementation Plan* on December 15, 2020. The *Implementation Plan* stressed collaboration with industry for promoting open architectures and open-source software for the 5G RAN and 5GC. By avoiding proprietary architectures and closed-source software, DoD hopes to encourage innovation and reduce cybersecurity vulnerabilities (DoD, 2020).

In contrast to domestic 5G users, DoD's mission requires it to operate outside the US. DoD anticipates leveraging the 5G networks of host nations in support of mission needs. However, firms with ties to the Chinese government (Huawei and ZTE) supply a significant portion of the 5G network infrastructure equipment outside US borders. The US government has recognized both Huawei and ZTE as national security threats (115th U.S. Congress, 2018; FCC, 2020a), while the UK government has identified inadequate cybersecurity controls in Huawei's software security engineering practices (HCSEC, 2019). Western 5G hardware suppliers face a competitive disadvantage against these companies, as the China-based firms enjoy subsidies from the Chinese government, and undercut their competition on price, allowing them to grow and maintain their global 5G infrastructure market share. The use of foreign 5G infrastructure containing Huawei or ZTE components presents DoD with security risks. These risks may originate from malicious hardware (backdoor or trojan) or vulnerable device firmware (whether created unknowingly or deliberately). DoD must also overcome vulnerabilities inherent in 5G network services (e.g., NFV, edge computing) APIs, or from 5G-connected IoT devices having inadequate security controls. The Implementation Plan advocates conducting security assessments to identify, assess, and alleviate these risks. These assessments are not limited to the RAN but include the 5GC (DoD, 2020).

On May 12, 2021, President Biden issued E.O. 14028 *Improving the Nation's Cybersecurity*, which advocated that the Government update its cybersecurity approach, moving from securing standalone systems to a zero-trust architecture utilizing secure cloud services (SaaS, IaaS, PaaS). It also reaffirmed the position that the Government and industry must work together to ensure the nation's cybersecurity, calling for the sharing of cyber threat intelligence between government agencies, information technology providers, and operational technology providers. While emphasizing the cybersecurity partnership between government and industry, it highlighted the latter's shared responsibility in achieving the objective: "The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace." (Biden, 2021)

E.O. 14028 also addressed supply chain security, directing the Secretary of Commerce to create secure software engineering guidance for vendors selling software systems to the Government. These guidelines are to pertain to secure software development practices and maintaining auditable records of the vendor's software development effort. They also request the vendor to supply a software bill of material (SBOM) for the system being procured.

On November 25, 2022 the FCC adopted a Notice of Proposed Rulemaking (FCC 22-84), titled *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program.* The corresponding rule went into effect on February 6, 2023 (FCC, 2023). This rule banned the importation of telecommunication network products produced by Huawei, ZTE, and certain other manufacturers for the purposes of resale or for use in US telecommunication networks. However, FCC 22-84 only prohibits the importation of complete devices (such as a femtocell's remote radio unit or baseband unit). The importation of components (such as a circuit board loaded with 5G firmware from a femtocell's baseband unit) for research purposes is not prohibited (Tannahill, 2023).

# **Threat Landscape**

The threat landscape of the 5G network overlaps with that of its predecessor wireless telecommunication networks (3G, 4G). Like previous generations of wireless technology, both the UE devices and the 5G WAPs could be attacked over their air interface. If left unattended, they could also be subject to physical tampering. However, there are some important differences in the consequences of an attacker's successful exploitation of a vulnerability in the 5G network versus earlier generations. These are caused by some of the

use cases for which 5G has been designed, such as support of the massive Internet of Things (MIoT) and network slicing.

The coming MIoT devices will use the 5G network to communicate. This will open a wireless attack vector that did not exist under 4G. The sheer number of such devices that will be connected to the 5G network constitutes a broad attack surface. Successful exploitation of vulnerable MIoT devices presents an opportunity for a DDoS attack on the 5G network (5G Americas, 2019). Perhaps more concerning, MIoT devices may have limited computing power and battery capacity due to form factor constraints. These limitations may preclude the use of strong encryption algorithms for communication with the 5G network, potentially making such devices less secure.

A compromised 5G WAP offers an attacker the ability to strike at both UEs connected to that WAP, and at the 5G Core network. Both could be achieved by leveraging features of the 5G network. For example, 5G overcomes one of the security vulnerabilities of 4G by never sending its subscriber information (Subscriber Permanent Identifier – SUPI) over the air unencrypted. Instead, it uses public key encryption to send an encrypted version of the SUPI, known as a Subscriber Concealed Identifier (SUCI). When a UE attempts to authenticate to the 5G network, it must authenticate to its home network (HN) by sending its SUCI through the serving network (SN) to its HN. If the HN authenticates the UE, it notifies the SN, and the device is permitted to connect to the network. This is an important difference from 4G authentication, which sent the subscriber's identity to the SN in the clear and did not require the UE to authenticate to the HN (Bhardwaj, 2020). Song, et al provide an overview of the differences between 4G and 5G authentication (Song, Xu, Tian, Chen, & Zhi, 2019). Graphical representations of 4G LTE and 5G authentication are presented in Figure 2 and Figure 3, respectively. For 5G authentication, the SUPI is encrypted into a SUCI using the public key of the subscriber's home network. This public key is installed on the UE by the home network provider, residing on an embedded universal integrated circuit card (eUICC). 5G key management provides that the HN have the capability to push an updated public key to the UE. In the case of a UE connected to a compromised 5G WAP, the WAP (such as a 5G small cell or femtocell) could push a malicious public key to the UE, preventing from authenticating to its HN, or permitting it to authenticate to a 5G "HN" controlled by the attacker. Previous research has shown that a malicious 5G WAP could also take advantage of

elements in the 5G authentication protocol to mislead a UE into revealing its SUPI (Jover & Marojevic, 2019).

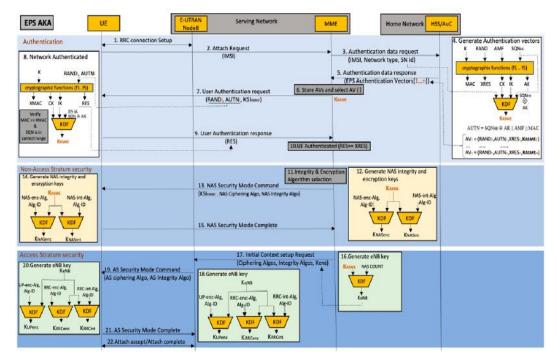


Figure 2: 4G LTE Authentication (Dhanasekaran, 2023)

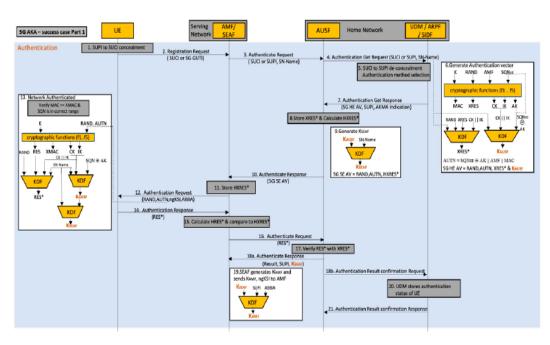


Figure 3: 5G Authentication (Dhanasekaran, 2023)

A malicious 5G WAP may be used to exploit vulnerabilities in the 5G Authentication and Key Agreement (AKA) protocol. Researchers have analyzed the 5G authentication and key agreement methods specified in the 3GPP 5G standard and have identified security vulnerabilities in the 5G AKA (Hu et al., 2019) and the Extensible Authentication protocol (EAP) AKA (called EAP-AKA') (Edris, Aiash, & Loo, 2022). These protocols are used for mutual authentication between the UE and the HN, and for setting up encryption. Because the UE and SN execute a portion of these protocols over the air interface prior to encryption of that connection, their transmissions could be subject to eavesdropping (passive attackers) and alteration (active attackers).

Attackers may also leverage a compromised 5G WAP to attack the 5G network itself. One of the features of 5G is "network slicing" (Zhang, 2019). This allows the network to be subdivided into "slices" offering different network services, latency, and bandwidth. While each slice may contain its own copy of a particular service, some services and resources are shared by all slices. A malicious WAP could be used to consume excessive resources in the slice it serviced, effectively causing a DoS attack for the user of that slice (Olimid & Nencioni, 2020). Alternatively, it could consume an excessive amount of the common resources, thus impacting other network slices (5G Americas, 2019).

#### CHAPTER 3: SYSTEM DESIGN (RESEARCH METHODOLOGY)

## Introduction

The purpose of this design science study was to support 5G network security by identifying vulnerabilities in femtocell firmware. It sought to achieve that objective by using static firmware analysis tools to search for vulnerabilities in firmware samples obtained from 5G femtocells. The strategy to fulfill the goals of this study was to construct and execute a research experiment following a Design Science methodology. This chapter presents the tactical details of how that was planned to be accomplished.

This chapter opens by describing the proposed research method and discusses the appropriateness of this method to the research problem. It then describes the structure of the research experiment as it was to be performed. The population of firmware samples is given, along with the rationale for their selection. The data collection procedures are presented, along with a justification for their selection, and their appropriateness for the chosen research method. The choice of research instrument (i.e., the experiment) is defended, and its applicability to the research problem is shown. The reliability of the research instrument is reviewed, including its internal and external validity.

The review of instrument validity is followed by a description of the data analysis techniques to be used. The basis for selection of particular techniques over alternative approaches, and their utility for the research method is presented. Topics pertaining to informed consent and Internal Review Board (IRB) issues do not appear, as this study does not involve human subjects. The chapter concludes with a summary.

#### **Research Methods and Design Appropriateness**

Four research methods were considered as candidates for this study's research methodology. These were *qualitative*, *quantitative*, *mixed methods*, and *design science*. Each of these methodologies has its own strengths and weaknesses. Because of this, all four methodologies may not be equally beneficial to the problem under study. When selecting a research methodology, it is imperative that the researcher consider the appropriateness of each method with respect to the type of study being conducted (Creswell & Creswell, 2017).

*Qualitative* research methods are appropriate for studies in the social sciences. Data for qualitative studies is often collected in surveys involving human subjects. The survey responses can be subjective (e.g., "mostly agree") leaving the researcher with the challenge of drawing generalizations from the set of survey responses (Creswell & Creswell, 2017). Generalizations are used within cases to infer characteristics of those particular cases (Goertz & Mahoney, 2012) which may not hold over the entire population. Study data may also be gathered from review of written documentation, visual media, audio recordings, and other sources which document human interactions with others (Saldana, 2011).

*Quantitative* research methods analyze the relationship between variables in the problem domain to test a theory. Unlike qualitative research methods which may yield subjective data, quantitative methods rely on *objective* values of the variables under consideration. These values are measured empirically, resulting in numeric data which can be manipulated by the application of statistical methods (Creswell & Creswell, 2017). In comparison to qualitative research methods, quantitative methods are used to analyze data across different cases to infer characteristics of study populations (Goertz & Mahoney, 2012).

*Mixed Methods* research employs a combination of quantitative and qualitative methods to collect the study data. By integrating both quantitative and qualitative data, the researcher may be presented with insights beyond those offered by exclusive use of either method (Creswell & Creswell, 2017). While the use of mixed qualitative and quantitative research methods may be viewed as combining different philosophies of data collection and interpretation (the subjective approach of qualitative methods versus the objective approach of qualitative methods). Some scholars disagree, viewing the differences between these two methodologies as the result of different underlying mathematical foundations (Goertz & Mahoney, 2012).

*Design Science* research is appropriate for the study of problems by means of evaluating an artifact in context by means of an experiment. The experiment evaluates the behavior of the artifact in the specified context. The design science methodology is applicable to two type of research questions, those being design problems (evaluation of proposed designs versus stakeholder goals) and knowledge questions (evaluation of observed behavior to answer questions about the research subject). The experiment is designed according to the type of design problem the researcher wishes to answer (Wieringa, 2014). Both qualitative and mixed qualitative-quantitative research methods were considered for this study but discarded due to their dependence on human subjects to provide qualitative responses to surveys (e.g., "somewhat agree", "strongly disagree"). While qualitative methods are used in social science research (Creswell & Creswell, 2017) they are difficult to apply to studies where the subject population consists of inanimate objects. Because the study subjects are object code, and not source code, attempts to perform the analysis by human inspection of the firmware would be prohibitively time-consuming. While decompilers such as Ghidra (Eagle & Nance, 2020) exist, and human analysis of the resulting source code could be attempted, the fidelity of the results would still be dependent upon the (arbitrary) skill level of the researcher. For these reasons, humans shall not be used to inspect the firmware samples for vulnerabilities. As this research does not use human subjects nor does it utilize human researchers to perform manual analysis on the subject population, the use of survey-based methods, such as qualitative (or mixed qualitative-quantitative) methods is not feasible.

As discussed in Chapter 1, the nature of the study (detection of vulnerabilities) implies that the analysis method maximizes code coverage to improve the fidelity of the results. This suggests that the firmware samples be analyzed by automated tools instead of by human researchers, as the analysis by manual means (e.g., human inspection of the firmware) would be prohibitively time-consuming. The use of automated analysis tools can be orchestrated by designing an experiment targeting their use with the subject population of firmware samples. Design Science was proposed as the research method for this study because it allows development of experiments to analyze the set of instructions comprising the firmware, and their sequence of execution. Performing research by an experiment uniquely designed to prove or disprove a hypothesis for the study's subject population further indicates Design Science as an appropriate research methodology.

Of the two types of Design Science research problems (design problems and knowledge questions) this study sought to answer a knowledge question. The study postulates a directional hypothesis, intending to prove  $H_1$  and disprove  $H_0$ . As such, it lent itself to a design science research methodology consisting of an experiment (Wieringa, 2014). To identify security vulnerabilities in femtocell firmware, the firmware must be analyzed, either by examining the corresponding source code, or at a lower level. As noted by Hou, firmware vulnerabilities are a direct consequence of vulnerabilities in the source code used to produce

that firmware (Hou et al., 2017). Automated source code vulnerability analysis tools are available to the research community. Although not exhaustive, the National Institute of Standards and Technology (NIST) maintains a list of such tools online (NIST, 2021). Despite the availability of these tools, they are not applicable to this study, as their use would require access to the source code used to generate the particular femtocell firmware samples being examined. However, this study anticipated that the required source code will be unavailable to the researcher. For this reason, the research was conducted by analyzing the firmware samples at the object code level.

The research design consisted of examining firmware samples from a set of 5G femtocell devices. Each device's firmware was subjected to analysis by multiple static analysis tools to identify vulnerabilities. Vulnerabilities thus identified were assigned a confidence rating based upon the number of analysis tools reporting the same occurrences. The potential for one or more tools to report false positive and/or false negative results does exist. However, the likelihood of these occurrences was minimized by using analysis tools proven by the research community and correlating their results to generate confidence ratings for identified vulnerabilities. Vulnerabilities reported on a manufacturer's femtocell firmware with a high degree of confidence would be supporting evidence for proof of  $H_1$  and would disprove  $H_0$  for that manufacturer. This "high degree of confidence" will be reinforced by the statistical power analysis provided by the G\*Power tool (see Chapter 3). Conversely, if no such vulnerabilities had been found (or only found with low confidence ratings)  $H_1$  would remain unproven (for that manufacturer), while the results would support  $H_0$  (but would not prove it, due to the small sample size in this study).

# **Population**

The population for this study was projected to be the set of 5G femtocells offered by Huawei, ZTE, Ericsson, Nokia, and Fujitsu. These manufacturers were selected because they possess the six largest shares of the global 5G equipment market (see Table 3). Larger 5G small cells, such as picocells, are excluded. 5G femtocells provide access to the 5G network by using a 5G radio interface and an IP-based backhaul connection (over the Internet) to the 5G network provider's 5G core network (Rodriguez, 2015a). They serve as a 5G WAPs for small numbers of users (residential femtocell: 4-8 users; enterprise femtocell: 16-32 users).

They are typically deployed in homes and buildings, to provide 5G coverage to indoor areas where signal strength from outdoor 5G WAPs would be attenuated by the building's walls and windows. As such, they are physically accessible to a malicious femtocell owner or other attacker. Recent estimates suggest that by 2021, approximately 70-80 percent of mobile data would be generated indoors (Cisco, 2020; Ericsson, 2021b). This implies that femtocells are likely to be ubiquitous in the deployed 5G network. For these reasons (ease of attacker access and ubiquitous deployment) femtocells present a broad 5G network attack surface.

Global suppliers of 5G femtocells are presented in Table 4. Note that none are based in the US. While time and budget constraints make it impractical to analyze the firmware of every 5G femtocell, this study examines the firmware from a cross-section of that population, to provide an indication of the vulnerabilities present. The current versions of each manufacturer's 5G femtocell products was determined by reviewing their corporate website, or by contacting their salespeople.

Manufacturer	Country of Origin
Huawei	China
Nokia	Finland
Ericsson	Sweden
ZTE	China
Samsung	South Korea
Fujitsu	Japan

Table 4. 5G Network Equipment Manufacturers, in Order of Global Market Share

# Sampling

The methodology used to select research subjects from a population is referred to as the *sampling design*. A sampling design may be *single stage* or *multistage*. In single stage sampling design, the identities of all members of the subject population are known to the researcher prior to the experiment. When that condition cannot be satisfied, the researcher may employ multistage sampling design. In multistage sampling, the researcher first partitions the population into groups, and selects a subset of those groups. For each group in the subset, the researcher determines the identity of each of its members, and creates a sampling from each group to serve as the research subjects (Creswell & Creswell, 2017). Multistage sampling is appropriate for populations whose membership is infeasible to identify completely (such as when the population of interest is very large). Multistage sampling is also called *cluster sampling*, due to the process of dividing the population into groups (clusters) in the first sampling stage (Babbie, 2020).

Both sampling designs may be implemented using one of three sampling types. If each member of the population has the same likelihood of being selected, the sampling process yields a systematic random sample. If the population has an ordering (such as an alphabetical ordering of names) a "precision-equivalent random sampling" may be generated by selecting an initial element of the population at random, and then selecting every Nth element from the ordered population. If neither form of random sampling can be generated, subjects may be selected simply because they are available while others are not. This is known as a "convenience sample" (Creswell & Creswell, 2017).

This study was anticipated to employ multistage sampling. In the first sampling stage, the 5G femtocell population was to be partitioned into clusters. The devices were to be clustered by manufacturer, as this forms a natural partitioning of the population. In the second sampling stage, a subset of the clusters was to be selected. That process was to be initiated by choosing a target number of research subjects (i.e., the 5G femtocell firmware samples) for the study. This number was anticipated to be in the range of 10-20. Then, starting with the Huawei cluster, clusters were to be selected one at a time, until the total number of members in all selected clusters met (or exceeded) the desired number of research subjects. The cluster selection order was to be Huawei, ZTE, Ericsson, Nokia, Samsung, and Fujitsu. Huawei and ZTE were to lead this ordering because their equipment has been determined to present national security risks (115th U.S. Congress, 2018; FCC, 2020a). The remaining manufacturer clusters were to be selected in decreasing order of their share of the global 5G device market. Ordering by global (instead of US) market share gives selection precedence to manufacturers whose 5G femtocells US cyber operators would be most likely to encounter overseas.

Once the group of clusters had been chosen, individual research subjects (i.e., femtocell firmware samples) would be selected from their members. The size of the Huawei

and ZTE clusters was limited due to restrictions on their deployment in the US. Notwithstanding that, the availability of devices for all clusters could have been limited by supply chain problems caused by the ongoing Covid-19 pandemic. Because of these uncertainties, it was anticipated that there may be fewer candidate research subjects than desired. Therefore, research subjects were to be selected from the clusters using a convenience sampling strategy (the elements comprising the sample will be chosen simply because they are available). However, should the total number of candidate research subjects in the selected clusters exceed the desired number of research subjects, they were to be selected in preference order. Put another way, if there were more candidate research subjects than needed for the study, the subjects were to be chosen in the order specified above. In that instance, all members of a given cluster (all firmware samples from a given manufacturer) were to be chosen before selecting any from the next cluster. The selections were to start from the Huawei cluster and continue through the clusters in order of decreasing precedence, using the same order used for cluster selection. Once all the Huawei samples have been added to the study, all the Nokia samples were to be added, then all the Ericsson samples, etc. until the desired number of research subjects had been included.

A target population may be sampled by *random sampling* (research subjects are selected randomly, with each element having the same probability of being selected), or by *stratified sampling*. To stratify a target population, a characteristic of its members is used to segment the population into strata. The study sample is then chosen by selecting members from each stratum of the population. In a truly stratified sampling, the size of each stratum in the selected sample is proportional to the size of that stratum in the target population. This sampling method provides a sample that more closely resembles the target population in the characteristic(s) of interest (those characteristics used to stratify the target population) than would result from a random sampling (Fowler, 2014). Conversely, if all characteristics of the target population were of equal interest, a random sampling method would be appropriate (Ernest, Geraldine, & Viktor, 2015).

To illustrate the concept of stratified sampling, suppose that a stratified sample was to be chosen from the set of integers that had been stratified by the property of being divisible by three. The set of integers and the resulting sample would each consist of two strata (those integers divisible by three, and those that are not). To create a truly stratified sample, exactly

42

twice as many integers would have to be selected from the "not divisible by three" stratum as those selected from the "divisible by three" stratum. The resulting sample would contain the same two strata as the target population, with the ratio of their cardinalities exactly mirroring the ratio of the corresponding strata in the target population.

A consequence of the proposed selection strategy was that the sample population would be *pseudo-stratified* by device manufacturer. The sampling algorithm gave precedence to manufacturers (i.e., strata) in order of their global 5G device market share (Fig. 1). Their market share serves as a rough approximation of their proportion of the target population. However, the ratios of the cardinalities of the resulting sample strata were unlikely to match their respective ratios in the target population. That phenomenon was caused by this study's device availability, time, and budget constraints. A summary of the pseudo-stratified selection algorithm is given below.

```
Lists of available firmware samples from: Huawei (H); Nokia (N);
Ericsson (E); ZTE (Z); Samsung (S); and Fujitsu (F).
N = Desired size of pseudo-stratified sample
P = List of firmware samples to be included in pseudo-stratified
sample population
A = List of available firmware sample lists, ordered by Huawei and
ZTE first, then in order of manufacturer market share
BEGIN
A = List(H, Z, N, E, S, F)
P = () /* empty list */, i = 0
WHILE ( P.size() < N ) AND ( i < A.size() ) DO {
    i = 0
    MFG = A_i
    WHILE ( P.size() < N ) AND ( j < MFG.size() ) DO {
        P.append(MFG<sub>1</sub>)
        j = j + 1
    }
    i = i + 1
}
```

END

Those same constraints were material to determining this study's sample size. While a large sample size may improve the accuracy of a study (Creswell & Creswell, 2017), this

study's constraints made it impractical to select a large sample from the target population. The limited availability of 5G femtocells in the marketplace necessarily constrained this research to sample only from those devices which could be obtained by the researcher. A preliminary online survey of new 5G femtocells indicated costs of approximately \$500 per device. As this research was funded solely by the personal funds of the researcher, the available budget restricted the upper limit of the sample size to 10 devices. If external funding had been obtained, that limit could be increased, however the maximum sample size would have still been constrained by the time available for the study. As this study was the work of an individual researcher, it is doubtful that even if funding to purchase additional devices became available, no more than 20 devices could be studied in a reasonable time. The possibility of extending this research by examining 5G femtocell devices not included in its selected sample will remain a challenge for future researchers.

# **Data Collection Procedures**

Each member of the research sample was be subjected to evaluation by each tool in the toolset *S*. Ideally, the number of tools (*T*) would be as large as possible, as the probability of all tools in *S* reporting a false negative,  $\epsilon$ , varies inversely with *T*. However, time constraints limited the value of *T* to no more than 20.

The Finite State Platform is a vulnerability analysis engine that is targeted to firmware analysis. It not only identifies vulnerabilities in firmware written by the device manufacturer, but it also detects vulnerabilities in the third-party components that are used. It can analyze compiled binaries and claims support for all instruction set architectures. Of importance to this study, it reports a list of all vulnerabilities (CVEs) identified, along with the software components in which they were found (Finite State, 2021). It has previously been used to analyze Huawei firmware (Finite State, 2019a). However, through email correspondence in January, 2022, Finite State declined to participate in this research, citing concerns regarding reproducibility and peer review of their proprietary algorithms (Wyckhouse, 2022).

Each tool in *S* was used to analyze all elements of the research sample which are of a type supported by that tool. It was unlikely that all tools in *S* would support the same set of firmware samples, but the members of *S* were chosen such that every element of the research sample is supported by at least one tool. For each run of a given tool Q, against an element *F* 

of the research sample a record was to be kept of the results reported by Q. This record was to have included, at a minimum, the fields indicated in Figure 4. The results for each run were to have been recorded in a Microsoft Excel spreadsheet, using one spreadsheet row per run, regardless of the number of vulnerabilities reported for that run. Each vulnerability reported by a given run was to appear in its own column on the row used to record that run.

	TOOL	SAMPLE	FIRMWARE	RUN DATE	/TIME	RUN DATE	TIME		os						
TOOL	VERSION	ELEMENT	VERSION	START		END		PLATFORM	VERSION	VULN 1	C1	VULN 2	C2	VULN 3	СЗ
								64-bit PC,	Linux	CVE-2021-		CVE-2018		CVE-2022-	
T00L-01	1.5	Nokia01	3.88	5/22/22	9:56 AM	5/23/22	10:10 A	1 32GB RAM	20.0	mmmmm	0.8	nnnnn	0.4	zzzz	1
								64-bit PC,	Linux	CVE-2021-		CVE-2022			
T00L-01	1.5	Nokia02	2.72	5/26/22	7:00 AM	5/26/22	8:18 A	1 32GB RAM	20.0	mmmmm	0.9	xxxxx	0.1		
								64-bit PC,	Linux	CVE-2021-					
T00L-02	2.0	Huawei01	3.88	5/24/22	1:21 PM	5/25/22	5:28 PI	1 32GB RAM	20.0	mmmmm	0.7				

Figure 4: Sample Results Spreadsheet

#### Validity

Creswell notes two types of threats to the validity of experimental studies, *internal* and *external*. Internal threats are those which mislead the researcher into using the results of the experiment to reach incorrect conclusions regarding the target population. External validity threats are those which mislead the researcher into using the results to reach incorrect conclusions about populations *other* than the target population from which the sample was drawn. Creswell lists 10 types of internal validity threats and three types of external validity threats (Creswell & Creswell, 2017).

Of the internal threat types listed by Creswell (Creswell & Creswell, 2017), eight regard changes in behavior or attitudes among human subjects, which was not a concern for this study, as femtocell firmware is inanimate. The remaining two (*selection*" and *"instrumentation*") were mitigated as follows. The *selection* internal threat is realized when the selection algorithm yields a research sample which is biased towards producing certain results. Admittedly, the convenience sampling algorithm described above is suboptimal for avoiding this threat. However, even if the selection algorithm resulted in a research sample whose level of vulnerabilities were not representative of the target population, the study results would still be valid. Those firmware samples with reported vulnerabilities are still considered to have them with a confidence rating of *C*. Those firmware samples with a confidence

rating of  $\epsilon$ . The *instrumentation* internal threat is realized when the study instrument changes during the study. This threat was to be mitigated by using only one version of each tool in *S* for the lifetime of the study.

Creswell presents three types of external validity threats (Creswell & Creswell, 2017). They are mitigated as follows. The *interaction of selection and treatment* external threat is realized when the characteristics of the research sample are insufficiently broad, preventing generalization to populations with broader characteristics. The mitigation for this threat was accomplished by the selection algorithm, which gives selection precedence to those femtocell samples from manufacturers with higher global 5G market share. Further mitigation could be performed by repeating the experiment on other (not previously selected) femtocell firmware, or on other 5G device firmware (such as 5G mobile phones). The *interaction of setting and treatment* external threat is realized when the nature of the research setting prevents generalization of the results to other settings. This threat was mitigated by the fact that the research subjects are firmware samples, not live entities, and as such are oblivious to changes in the research setting. The *interaction of history and treatment* external threat is realized when the nature of the study prevents its results from being valid at any time other than when the study was conducted. This threat was mitigated by the time-independent nature of the results, and the deterministic nature of software execution.

The National Academy of Sciences notes that the definitions of a study's reproducibility and replicability vary across research disciplines (National Academies of Sciences & Medicine, 2019). This study has adopted the definitions proposed by the Association of Computing Machinery (ACM) (ACM, 2020). This study was anticipated to be *reproducible* under these definitions. That is, other researchers repeating this study (possibly at a different location) using the same tools and tool versions in *S* with the same femtocell firmware samples as used in the original study can be expected to produce the same results. Should the same results not be found, some possible causes of the discrepancies include changes to the analysis algorithms used by the tools, and classification of new CVEs by MITRE since the tools were last executed on the sample population.

However, attempts to repeat this study varying the tools in *S* (or different versions of the same tools found in *S*), or varying the femtocell firmware samples or versions used in the original study may yield different results. Therefore, this study might not be *replicable*,

meaning that the results of the study are dependent upon the particular tools, tool versions, and datasets used to conduct the study.

A further validity threat may be found in the constraints on the researcher conducting the study. In academia, researchers are sometimes under employment-related pressure to produce a certain volume of scholarly literature. This "pressure to publish" can lead some researchers to compromise the reproducibility and replicability of their studies in an effort to accelerate completion and achieve a higher annual publication rate. The author of this study was not employed by any organization which requires publications in academic literature, mitigating the potential threat to the reproducibility and replicability of this study.

#### **Data Analysis**

Data analysis is the process of examining the results of the study (the data) to produce useful information. The data from this study supported the generation of a set of metrics for the research sample, calculated as follows. *Most Vulnerable Firmware* ( $M_1$ ): the sample with the highest number of reported CVEs. *Most Likely Exploitable Firmware* ( $M_2$ ): the sample having the CVE with the highest value of *C*, calculated by the formula given in Chapter 1. *Most Insecure Manufacturer* ( $M_3$ ): the manufacturer (stratum) having the highest percentage of samples for which at least one CVE has been found. *Most Common CVE* ( $M_4$ ): the CVE with the highest number of occurrences across all firmware samples. These metrics were selected to support decision making by 5G femtocell stakeholders, cyber defense professionals, and offensive cyber operations planners. This set of metrics was not closed. The inclusion of additional metrics was considered prior to completion of the study. The assignment of new tools to set *S* might also have supported the creation of additional metrics. This initial set of metrics was chosen over statistical measures due to the limited size of the research sample. Given a sample size of 20 or fewer elements, statistical measurements such as arithmetic mean or variance are unlikely to be meaningful.

# **Chapter Summary**

This chapter discussed the research method selected, describing this study as a design science quasi-experiment intending to prove a directional hypothesis. The target population of

the study and the pseudo-stratified research sample selection algorithm were presented. The inapplicability of informed consent to this study was noted. Data collection methods and tools were described. The use of a quasi-experiment was then justified, along with a discussion of its reliability. That was followed by the topics of internal and external validity threats and their mitigation. This chapter closes by presenting the data analysis artifacts that were to be constructed from the study results, and their method of computation. The study results themselves, and the computed values of the metrics, are presented in Chapter 4.

# **CHAPTER 4: RESULTS**

## Introduction

This study intended to determine if 5G femtocell firmware from Huawei, ZTE, and other major manufacturers of 5G networking equipment contained vulnerabilities. It determined the presence of vulnerabilities by scanning the firmware with multiple SAST tools. Difficulties encountered in procurement of firmware samples and access to SAST tools resulted in the study being executed differently than planned. Despite these obstacles, the study was completed, and the research objective was achieved.

# **Firmware Procurement**

The procurement of firmware samples proved to be much more difficult than anticipated. The anticipated availability of 5G femtocell firmware freely downloadable from manufacturer websites proved to be a fallacy. During this study, attempts were made to obtain firmware from Huawei, ZTE, and Nokia websites. None of these made firmware downloads accessible to parties who were not MNOs and did not have an existing relationship with the manufacturer. An attempt was made to obtain Huawei firmware via a "friend of a friend" contact at an MNO (Viva-MTS) located in a foreign nation where the use of Huawei equipment had not been prohibited. That effort was unsuccessful, due to a language barrier and logistical considerations. The inability to obtain firmware samples via download threatened the viability of this study. To overcome this obstacle, it was decided to obtain the firmware indirectly, by procuring 5G femtocell hardware, and then copying its firmware directly from its onboard storage. That approach presented its own set of challenges.

Several vendors of 5G small cell products were contacted to purchase 5G femtocells. Each of these efforts was unfruitful. The reasons for this lack of success varied from vendor to vendor but fell into three general categories. First, some vendors did not offer a 5G femtocell product. This sometimes occurred even with vendors whose websites claimed that they offered such a product. Their sales representatives would state that the femtocell product in question was still under development or was still awaiting FCC approval. Second, some vendors refused to sell their products to an individual. They limited their sales to MNOs only. This limitation was also encountered when inquiring directly with major manufacturers (e.g., Nokia). Examples of vendor replies are quoted below. They are representative of the type of vendor responses received. The full text of these messages is shown in Appendix B (Figure 16 through Figure 21).

CommScope does not offer a 5G femtocell, and even if they did, they would only sell it to their partners and MNOs.

"Hi Charles, sorry for the delayed response. For clarification CommScope does not offer a femto product. Our OneCell product is a small cell cloud RAN product designed for the Enterprise market with a connection capacity of 1024 users. In addition, our OneCell product is only purchased by our certified partners or directly by the MNO. Our contractual agreement(s) with the Operator(s) require us to offer our small cell only through these channels to ensure the Operators licensed 4G and 5G spectrum is deployed accordingly. Unfortunately, we are not able to offer you our OneCell small cell product for your effort." (Sbisa, 2022)

Crown Castle did not offer a 5G femtocell, but still wanted to know if there was a possibility of selling enough units to provide 5G coverage for the DSU campus.

*"We do not have these devices. Are you interested in improving the cell coverage on the campus or are you just doing some research?" (Thompson, 2022)* 

Citing supply chain limitations, Accuver was unwilling to sell only a single unit.

"My apologies fot [sic] the delay in response. Unfortunately, I received word from our HQ that they are unable to sell just one small cell. We don't have a stock here in the US and our HQ is focusing on large scale opportunities based on meeting a certain MoQ with our factory." (Ostien, 2022)

The third reason for being unable to purchase these products was the stated intention to use them for university cyber research. When conversing with some sales representatives, when the term "research" was mentioned, the tone of the conversation cooled. Even offering to sign an NDA and anonymize their product in the research results failed to facilitate a purchase. The vendor staff who were contacted appeared to be interested exclusively in sales of multiple units. The advancement of knowledge in the field of cybersecurity was insufficient motivation for them to loan out a unit even temporarily for research (that appeal was made, but to no avail). A sampling of purchase attempts and their reasons for failure are given in Table 5.

Vendor	Reason for not completing sale
Actiontec	Only sells to MNOs.
Accuver	Would not sell just one unit.
BTI Wireless	5G Femtocell not FCC certified yet.
Airspan	Only sells to MNOs.
Communications	
Askey Computer	Emails to vendor unanswered. Calls to the
Corp.	US sales office in California and to
	company headquarters in Taipei, Taiwan
	were not answered.
Commscope	No femtocell product. Only sells to MNOs.
Crown Castle	No femtocell product.
Ericsson	Only sells to MNOs
Mavenir	Only sells to MNOs
Systems	
Nokia	Only sells to MNOs
SerComm	Would not sell to a researcher.
Sterlite	Would not sell just one unit.
Technologies	

Table 5: 5G Femtocell Purchase Attempts

A further difficulty was caused by the restrictions placed on the researcher, due to the nature of his employment. These restrictions prohibited the researcher from making direct contact with Huawei and ZTE, due to their designation as national security threats. As the 5G femtocell products of these two manufacturers were primary targets of this research, these

restrictions negatively impacted the ability to obtain information from Huawei and ZTE. This inability to obtain detailed information on the Huawei Lampsite and ZTE Qcell 5G indoor small cell products initially led the researcher to expend part of the research budget on the purchase of Huawei and ZTE remote radio units (RRUs) for these products. The RRUs were not purchased directly from Huawei or ZTE due to the restrictions noted above. Instead, they had been purchased on Alibaba.com through Dakota State University (to obscure the identity of the researcher).

During attempts to extract firmware from these units, it was discovered that they did not contain the firmware which controlled the femtocell. Rather, they were to download their firmware from a connected baseband unit (BBU). As the RRUs were new devices which had not been previously connected to a BBU, their firmware had not yet been downloaded. Given the restrictions on the researcher mentioned previously, contacting Huawei or ZTE in China was not possible. Therefore, the researcher contacted Huawei North America (in Texas) using a "burner" mobile phone and an assumed name. To identify the proper firmware version for the Huawei RRUs, the Huawei North America representative requested their serial numbers. When this information was provided, the representative refused to provide any support information, citing the fact that they had not been purchased directly from Huawei. Contacting ZTE's North American support site (again with the burner phone and assumed name) also failed to obtain the required firmware. In the ZTE case, the serial number of the RRU indicated that it was a "China only" unit and was not to have been exported. The representative became agitated upon discovery of this fact and refused to provide further assistance. Without firmware, the RRUs were of no value to the research effort. They were donated to Dakota State University.

The quest to obtain 5G femtocell hardware from which firmware could be extracted now concentrated on purchasing Huawei and ZTE BBUs. Leveraging lessons learned from the RRU procurement, used BBUs were targeted for purchase as they would already have been loaded with firmware. While these could be purchased online from websites such as Alibaba.com, there was uncertainty surrounding their ability to be imported. At that time (January 2023) FCC Rule 22-84 had been proposed but had not yet taken effect. It was still possible that the Rule might be revised to further restrict importation. To mitigate the risk of being unable to import the BBUs, the possibility of importing them into Canada, extracting

the firmware samples on Canadian territory, and then bringing only the samples into the US was considered. However, consultation with the Canadian Innovation, Science, and Economic Development office (Desmaris, 2023) revealed that importation of Huawei and ZTE equipment into Canada would not be possible, due to a ban by the Canadian Government (Sevastopulo & Kerr, 2022).

Successful importation of Huawei and ZTE BBUs into the US depended upon the details of FCC Rule 22-84 when it reached its final form. The initial attempt to obtain a clarification of Rule 22-84 from the FCC was unsuccessful. However, less than 48 hours after enlisting the assistance of US Senator Marco Rubio's office, the FCC provided a knowledgeable person (Mr. George Tannahill, of the FCC Office of Engineering and Technology Laboratory) who was able to clarify the provisions of Rule 22-84 as it pertained to this research (Repasi, 2023). Per the explanation of Rule 22-84 provided by Mr. Tannahill, the importation of complete units (such as an entire BBU) would be prohibited, but the importation of *components* (such as a BBU baseband board or switching board) would still be permitted. An excerpt from Mr. Tannahill's email message is provided below. The full text appears in Appendix B (Figure 19). The FCC's letter documenting their provision of this assistance appears in Appendix B (Figure 20).

"The FCC released FCC <u>22-84</u> on November 25, 2022 related to prohibiting equipment authorization of specific devices produced by entities identified on a <u>covered list</u> that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. When the rules become effective upon publication in the Federal Register, FCC 22-84 will prohibit new equipment authorizations for specific equipment produced by entities named on the covered list. Huawei and ZTE are both entities named on the covered list." (Tannahill, 2023)

The 5G firmware analyzed in this study was extracted from used BBU components obtained from Alibaba.com (<u>https://www.alibaba.com</u>) and from a professional contact, Mr. Earl Lum (<u>https://www.ejlwireless.com</u>). A total of nine used BBU boards were purchased from Alibaba.com. While the various equipment resellers were able to provide used hardware

(containing the 5G firmware) they were not able to sell Huawei or ZTE software/firmware by itself, citing Huawei's "restrictions" on export of their software, as shown in Figure 5.

chengyu chen 2023-01-16 20:21

С

Hi, I'm sorry, my friend. I asked all our channel partners that Huawei's 5900 can only solve the problem of hardware, but we cannot export the software for the time being. Due to Huawei's restrictions, we can get high prices for other brands, and there are not many products available.

#### Figure 5: Huawei restricts export of software.

The Alibaba.com purchases were made by creating an account on that website (https://www.alibaba.com) and posting RFQs for the type and quantity of equipment needed. Replies from several China-based suppliers were received within 24 hours of an RFQ being posted. Costs for each board ranged from \$373 to \$717, including shipping from China to Florida, USA. Sales were arranged via the website. Vendor communication was initiated via the website but was occasionally followed by email communications. These interactions sometimes gave insight into the business ethics of particular Alibaba.com suppliers. For example, the quotation below is from an Alibaba.com supplier who was willing to disassemble and "white label" a Huawei 5900 BBU to circumvent the restrictions of FCC Rule 22-84. The full text of the email appears in Appendix B (Figure 21).

"Yes, we can split to some parts and send to you. In addition, change the brand name is also possible. What is your quantity? Do you only want the second hand?" (Hebei Shencheng, 2023)

A total of nine used BBU boards were purchased through Alibaba.com. Of these nine, four were Huawei 5900 BBU components, four were ZTE ZXRAN V9200 BBU components (ZTE, 2020), and one was a Nokia AirScale BBU component (Nokia, 2019). Each board had previously been loaded with Huawei 5G RAN, ZTE ZXRAN, or Nokia 5G RAN firmware. The total cost for these boards was approximately \$4000. The boards sourced from Alibaba.com appear in Table 6. A representative board (ZTE VSWd1) is shown in Figure 6.

Manufacturer	Model	Туре
Huawei	UBBPg2a1	5G baseband board
Huawei	UBBPg3	5G baseband board
Huawei	UMPTe3	5G BBU controller board
Huawei	UMPTg3	5G BBU controller board
Nokia	5G Flexi ABIA 473906A	5G baseband board
ZTE	VBPd0b	5G baseband board
ZTE	VSWc2	5G BBU controller board
ZTE	VSWd1	5G BBU controller board
ZTE	VSWd2	5G BBU controller board

#### Table 6: 5G BBU boards sourced from Alibaba.com.



Figure 6: ZTE VSWd1 BBU controller board from Alibaba.com.

Three additional boards were provided on loan from a professional contact, Mr. Earl Lum. Mr. Lum is a researcher and published author on small cell technology and communication hardware components (Lum, 2023). Of these three boards, only one was selected for inclusion in this study. The selected board was the memory module of an Ericsson BB6648 baseband board, loaded with Ericsson 5G RAN firmware (Figure 7).



Figure 7: Memory Module from Ericsson BB6648

# **Firmware Extraction**

Once the BBU boards were received, the next challenge that faced the study was the problem of how to extract copies of the firmware. While this study's author does have some hardware experience, the specialized knowledge required to perform the firmware extraction exceeded his level of expertise. An Internet search located Mr. Xiaodong Zou (Figure 8) a resident of Toronto, Canada. Mr. Zou had performed reverse engineering on similar hardware (Huawei 4G BBUs). He was contacted via email, and recommended desoldering individual chips from the BBU boards, and reading them with a chip programmer. The tools and expertise necessary for such an approach were not available for this study.

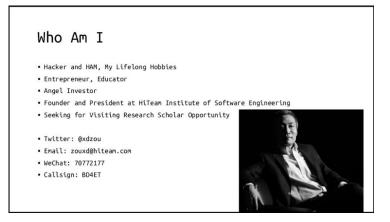


Figure 8: Xiaodong Zou

Dakota State University does not currently have an Electrical Engineering department, necessitating seeking firmware extraction resources from external sources. The required expertise was located at a local research university, the University of South Florida (USF). The USF main campus is approximately 27 miles from the location where this study was conducted, allowing for convenient delivery of the BBU boards. The USF Electrical Engineering department offered the services of Dr. Alex Otten (Otten, 2023). Dr. Otten successfully extracted the firmware from five memory modules on the BBU boards. Two of these (eUSB and NVMe drive firmware) were taken from the ZTE VSWd1 (Figure 9), and one from each of the ZTE VSWc2 (Figure 10), ZTE VSWd2 (Figure 11), and Ericsson BB6648 BBU (Figure 7) boards.



Figure 9: ZTE VSWd1 controller board.

# ZTE VSWc2

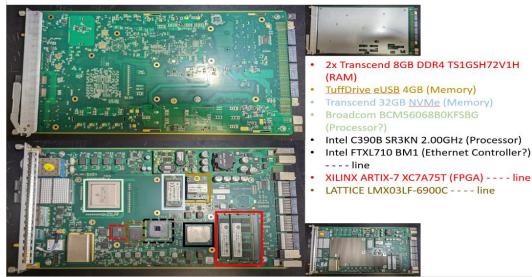


Figure 10: ZTE VSWc2 controller board

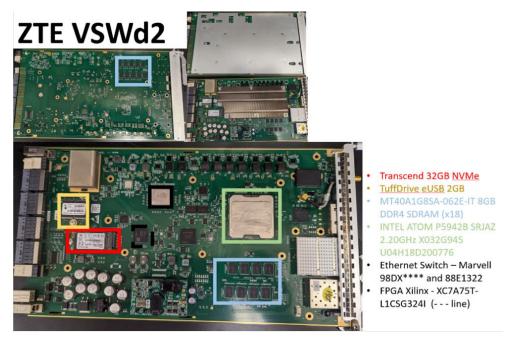


Figure 11: ZTE VSWd2 controller board

Firmware extraction from the Huawei boards proved to be problematic. Per Xiaodong Zou's suggestion, the memory modules were to be desoldered from the boards. This proved impossible for the Huawei UMPTg3 BBU controller, as its memory modules were potted to the board with epoxy (Figure 12). Whether this was done by Huawei or by the Alibaba.com supplier in an effort to thwart reverse-engineering of the board is not known. In either case, the part numbers of the memory modules had been etched off, making them unidentifiable. The memory modules of the remaining Huawei boards and the Nokia Flexi ABIA board were successfully desoldered, but the firmware could not be read.

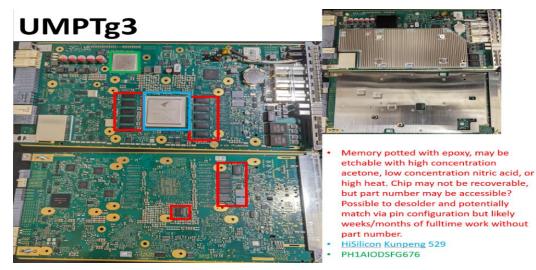


Figure 12: Huawei UMPTg3 with epoxied memory modules

The five firmware samples captured by the extraction effort were used as the sample population for this study. While this small sample size was below the goal of 16 samples outlined in Chapter 3, time and budget constraints prevented the acquisition of additional 5G femtocell hardware.

## **SAST Tool Selection and Scan Procedure**

As noted in Chapter 1, open-source tools were initially considered for this study. However, as the study progressed, it became clear that they did not have the capacity to scan the samples and report vulnerabilities at the level desired for this study. In particular, the CPPcheck (Sourceforge.io, 2023) and Joern (Joern.io, 2023) tools were considered for use but rejected. The primary reasons for their rejection were their lack of ability to process firmware samples of the sizes needed for this study, and their insufficiently detailed reporting capability for CVEs identified in those samples. Therefore, the decision was made to eschew the use of open-source tools and perform the study by using commercial SAST tools (CSTs).

Chapter 1 presented the four CSTs used for this study, and their version identifiers (Table 2). In keeping with the intention to use NIST-recognized tools as stated in Chapter 1, note that Grammatech Code Sentry® is on the NIST list of source code security analyzers and Synopsys Black Duck Binary Analysis® incorporates their Coverity® tool, which appears on the same NIST list. Blackberry Jarvis® is included in the NIST list of binary code scanners. The Finite State Platform is not currently on either NIST list.

The online versions of each tool were used to perform vulnerability scans. All scans were performed using each tool's default configuration. Each of the five firmware samples were uploaded to each tool for analysis. To decrease the upload time, each sample was compressed into a zip file prior to uploading. The tools unzipped each file before performing their scans. The unzipped samples were scanned "in the cloud" with scan time varying between a few minutes and 24 hours (for the largest sample). Each scan generated several reports for each firmware sample. The reports were downloaded and form the set of artifacts for this study. While the presentation format of the findings varied between tools, at a minimum all tools created a software bill of materials (SBOM) and a list of CVEs for each component found in the sample.

## **Firmware Scan Results**

This section describes the salient scan results reported by the CSTs. The sheer volume of results made full inclusion of the scan reports impractical. For example, one tool produced 14 individual reports, varying in length from a single page to over 500 pages. Another produced only five reports, but the summary scan report was a PDF file over 1200 pages in length. Summaries of each scan are presented here, with a discussion of the results for each sample. The complete results from each scan are available for Committee review at a URL provided by DSU. Each firmware sample was assigned an arbitrary identifier to obscure the provenance of the samples from the CST vendors, to eliminate the chance of such information biasing the scan results. The list of firmware samples, their sizes, and identifiers is given in Table 7.

Sample	Firmware	Size	Zipped
Identifier			(upload) Size
C1	ZTE VSWd1 NVMe drive	5.54GB	3.60GB
C2	ZTE VSWc2 NVMe and TuffDrive drives	2.59GB	1.13GB
C3	ZTE VSWd2 NVMe and TuffDrive drives	6.51GB	4.19GB
C4	ZTE VSWd1 eUSB drive	455MB	305MB
C5	Ericsson BB6648 entire drive	7.6GB	65MB

Table 7:	Firmware	samples,	sizes,	and	identifiers.
----------	----------	----------	--------	-----	--------------

#### **C1 Scan Results**

All four CSTs in set *S* successfully produced scan reports for firmware sample C1. The scan results appear in Appendix C. Due to space limitations, only excerpts of the full reports are presented. The full reports are accessible to the Committee at a URL provided by DSU. The full list of all CVEs identified in sample C1 are given on the "C1" sheet the *statistics.xlsx* file, which is available to the Committee at a URL provided by DSU.

The Black Duck scan reports (Figure 23 through Figure 32) identified the presence of 67,458 CVEs, of which 1,831 were unique. The Code Sentry scan reports (Figure 33 through Figure 35) identified the presence of 2,045 CVEs, of which 1,962 were unique. The Jarvis scan reports (Figure 36 through Figure 44) identified the presence of 1,182 CVEs, of which 586 were unique. The Finite State Platform scan reports (Figure 45 through Figure 48)

identified the presence of 147 CVEs, of which 49 were unique. When the resulting 4,428 unique CVEs which were identified by at least one CST were examined, 3,524 of those were found to be unique.

#### **C2 Scan Results**

Three of the four CSTs in set *S* successfully produced scan reports for firmware sample C2. The Code Sentry tool produced only a partial scan report. The scan results appear in Appendix D. Due to space limitations, only excerpts of the full reports are presented. The full reports are accessible to the Committee at a URL provided by DSU. The full list of all CVEs identified in sample C2 are given on the "C2" sheet the *statistics.xlsx* file, which is available to the Committee at a URL provided by DSU.

The Black Duck scan reports (Figure 49 through Figure 59) identified the presence of 20,633 CVEs, of which 2,159 were unique. The Code Sentry scan reports (Figure 60 through Figure 62) failed to produce a report containing CVE details. The Jarvis scan reports (Figure 63 though Figure 70) identified the presence of 1,352 CVEs, of which 845 were unique. The Finite State Platform scan reports (Figure 71 through Figure 74) identified the presence of 130 CVEs, of which 61 were unique. When the resulting 3,065 unique CVEs which were identified by at least one CST were examined, 2,389 of those were found to be unique.

#### C3 Scan Results

All four CSTs in set *S* successfully produced scan reports for firmware sample C3. The scan results appear in Appendix E. Due to space limitations, only excerpts of the full reports are presented. The full reports are accessible to the Committee at a URL provided by DSU. The full list of all CVEs identified in sample C3 are given on the "C3" sheet the *statistics.xlsx* file, which is available to the Committee at a URL provided by DSU.

The Black Duck scan reports (Figure 75 through Figure 85) identified the presence of 76,561 CVEs, of which 1,814 were unique. The Code Sentry scan reports (Figure 86 through Figure 89) identified the presence of 2,302 CVEs, of which 2,216 were unique. The Jarvis scan reports (Figure 90 through Figure 98) identified the presence of 1,776 CVEs, of which 1,246 were unique. The Finite State Platform scan reports (Figure 99 through Figure 102) identified the presence of 147 CVEs, of which 49 were unique. When the resulting 5,325

unique CVEs which were identified by at least one CST were examined, 3,759 of those were found to be unique. Interestingly, the Finite State Platform reported *exactly the same set of CVEs* (and the same set of unique CVEs) for sample C3 as it did for sample C1. This occurred even though sample C1 consisted of the contents of an NVMe drive alone, while sample C3 included the contents of both an NVMe drive *and* a TuffDrive. All other CSTs reported differences in the CVEs reported for samples C1 and C3. The cause of the Finite State Platform's reporting identical CVEs for samples C1 and C3 could not be determined and remains a question for future researchers.

#### C4 Scan Results

All four CSTs in set *S* successfully produced scan reports for firmware sample C4. The scan results appear in Appendix F. Due to space limitations, only excerpts of the full reports are presented. The full reports are accessible to the Committee at a URL provided by DSU. The full list of all CVEs identified in sample C4 are given on the "C4" sheet the *statistics.xlsx* file, which is available to the Committee at a URL provided by DSU.

The Black Duck scan reports (Figure 103 through Figure 113) identified the presence of 9,725 CVEs, of which 1,918 were unique. The Code Sentry scan reports (Figure 114 through Figure 117) identified the presence of 1,990 CVEs, of which 1,329 were unique. The Jarvis scan reports (Figure 118 through Figure 126) identified the presence of 1,030 CVEs, of which 967 were unique. The Finite State Platform scan reports (Figure 127 through Figure 130) identified the presence of 70 CVEs, of which 49 were unique. When the resulting 4,263 unique CVEs which were identified by at least one CST were examined, 3,130 of those were found to be unique.

#### C5 Scan Results

Two of the four CSTs in set *S* successfully produced scan reports for firmware sample C2. The uncompressed size of sample C5 (7.6GB) exceeded Code Sentry's maximum sample size, causing the scan to fail. The Finite State Platform's scan never completed and required manual intervention to terminate. The scan results for Black Duck and Jarvis appear in Appendix G. Due to space limitations, only excerpts of the full reports are presented. The full reports are accessible to the Committee at a URL provided by DSU. The full list of all CVEs

identified in sample C5 are given on the "C5" sheet the *statistics.xlsx* file, which is available to the Committee at a URL provided by DSU.

The Black Duck scan reports (Figure 131 through Figure 141) identified the presence of 1,015 CVEs, of which 733 were unique. The Code Sentry scan reports (Figure 142 through Figure 145) failed to produce a report containing CVE details. The Jarvis scan reports (Figure 146 through Figure 154) identified the presence of 1,071 CVEs, of which 1,065 were unique. The Finite State Platform failed to produce a scan report. When the resulting 1,798 unique CVEs which were identified by at least one CST were examined, 1,377 of those were found to be unique.

#### **Confidence Measurements and M1-M4 metrics**

The four CSTs successfully detected multiple CVEs in samples C1-C5. The count of unique CVEs reported by each CST is given in Table 8. This data is sufficient to disprove  $H_0$  (by counterexample) but is only implicative evidence (i.e., it is not sufficient to prove)  $H_1$ . There were only four tools in set S (T = 4). This was significantly fewer than the number of tools anticipated to be available for the study. The small size of T may have reduced the reliability of the confidence rating, C. The number of unique CVEs identified in each sample, ordered by C, are given in Table 9.

Sample	Number of Unique CVEs			
	Identified in Sample			
C1	3524			
C2	2389			
C3	3759			
C4	3130			
C5	1377			

Table 8: Number of Unique CVEs Identified in each Sample

#CVEs	C1	C2	C3	<b>C4</b>	C5
with C:					
1.00	6		5	1	
0.75	148	16	377	258	
0.50	590	644	797	614	421
0.25	2780	1729	2580	2257	954

Table 9: CVE findings C values

The study results were also impacted by two of the CSTs being unable to provide results for certain members of the sample population. Specifically, Code Sentry successfully completed its scan of C2, but crashed when attempting to produce its scan report (a PDF file) due to the number of generated pages exceeding an undefined threshold. Code Sentry also failed to scan sample C5, due to the size of C5 (7.8GB unzipped) exceeding Code Sentry's maximum sample size (7GB). The Finite State Platform's attempt to scan sample C5 resulted in an infinite loop. No results were produced. These scan failures impacted the statistics for C2 and C5, as they were computed with smaller values of T (T = 3 and T = 2, respectively) than C1, C3, and C4 (T = 4 for each).

Chapter 3 introduces four metrics ( $M_1$ - $M_4$ ) to be determined by the study. These metrics were computed as follows. The metric  $M_1$  was found by determining the study sample for which the highest number of CVEs were identified. From Table 8, we find that  $M_1 = C3$ . Metric  $M_2$  was determined by selecting the sample with the highest number of CVEs having a C value of 1.0.  $M_2 = C1$ , as shown in Table 10. The metric  $M_3$  was not meaningful, as difficulty in firmware extraction prevented harvesting samples from the Huawei and Nokia hardware which had been purchased for this study. Thus, the number of manufacturers represented in the sample population was reduced to two. The  $M_4$  metric (the CVEs most identified by the set of CSTs) represented a set of 454 CVEs which were identified by *at least one* tool in every one of the samples (C1-C5). A full listing of all the CVEs detected, unique CVEs detected, the CVEs comprising  $M_4$ , the C values, as well as supporting evidence for the calculation of the other metrics can be viewed in the file statistics.xlsx at a URL provided by DSU.

Sample	Number of CVEs
	having $C = 1.0$
C1	6
C2	0
C3	5
C4	1
C5	0

Table 10: Number of CVEs per sample having C = 1.0

#### **Common Vulnerabilities Detected Across All Firmware Samples**

Metric  $M_4$  represented a set of 454 CVEs which were common across all firmware samples. This may indicate the use of common libraries and/or operating system versions across samples C1-C5. While some commonality might be expected in samples from the same manufacturer (samples C1-C4 were taken from ZTE products) that cannot explain the presence of the same 454 CVEs in sample C5 (an Ericsson sample). Analysis of the CVEs as described in NIST's National Vulnerability Database (NVD) partitioned the 454 common CVEs into 25 groups (Table 11). An explanation of the groupings follows.

AMD CPU: CVEs specific to the behavior of certain AMD CPUs (e.g., CVE-2021-26341).

*Android kernel:* Some CSTs reported CVEs related to the Android kernel (e.g., CVE-2021-0605). This is a surprising result, as all the femtocells in this study used versions of the Linux operating system. These CVEs may be false positives.

*ARM microprocessor:* CVEs specific to the behavior of certain ARM microprocessors (e.g., CVE-2022-33744).

*Bluetooth:* CVEs related to Bluetooth support (e.g., CVE-2020-26555). Whether the femtocells actually support a Bluetooth interface is unknown.

*BusyBox:* CVEs present in the versions of BusyBox included in the firmware (e.g., CVE-2018-1000500).

*bzip2:* CVEs present in the versions of bzip2 included in the firmware (e.g., CVE-2016-3189).

*curl:* CVEs present in the versions of curl included in the firmware (e.g., CVE-2020-8177).

*E2fsprogs:* CVEs present in the versions of e2fsprogs included in the firmware (e.g., CVE-2022-1304).

*Expat (libexpat):* CVEs present in the versions of libexpat included in the firmware (e.g., CVE-2022-22822).

*False positives:* These CVEs were identified in the CST scans, but their entries in the NVD indicate that they are not true vulnerabilities (e.g., CVE-2022-23816). Therefore, the CVEs in this group are all false positives. Further, it indicates that the CSTs will report CVEs whose entries have a status of "REJECTED" in the NVD (i.e., they are false positives).

*glibc*: CVEs present in the versions of glibc included in the firmware (e.g., CVE-2022-23218).

*Intel driver:* CVEs present in the versions of the Intel device drivers included in the firmware (e.g., CVE-2019-0136).

*Intel CPU:* CVEs specific to the behavior of certain Intel CPUs (e.g., CVE-2019-0154).

*Linux kernel:* CVEs present in the versions of the Linux operating system used by the firmware (e.g., CVE-2019-0136). This category alone accounted for 47.6% of the 454 common CVEs.

*Ncurses:* CVEs present in the versions of ncurses included in the firmware (e.g., CVE-2018-19211).

*NETGEAR:* CVEs related to NETGEAR devices (e.g., CVE-2020-15436). The reason for the presence of NETGEAR-related files in the firmware samples is unknown. CST reported CVEs in this category may be false positives.

*OpenSSH:* CVEs present in the versions of OpenSSH included in the firmware (e.g., CVE-2020-15778).

*OpenSSL:* CVEs present in the versions of OpenSSL included in the firmware (e.g., CVE-2020-1971).

*Other:* A set of eight CVEs which were not included in any other category. These CVEs were: CVE-2014-2524, CVE-2019-9503, CVE-2019-18276, CVE-2019-20795, CVE-2020-4788, CVE-2020-25656, CVE-2022-1271, CVE-2022-3715.

*PCRE (libpcre):* CVEs present in the versions of libpcre (regular expression processing) included in the firmware (e.g., CVE-2017-11164).

*Shadow:* CVEs present in the versions of shadow included in the firmware (e.g., CVE-2023-29383).

*Wi-Fi:* CVEs present in the code providing Wi-Fi Protected Access features (e.g., CVE-2020-24586). Whether the femtocells actually support a Wi-Fi interface is unknown.

*Windows 10 driver:* CVEs present in ALFA Windows 10 driver 6.1316.1209 included in the firmware (e.g., CVE-2020-26140).

*Xen:* CVEs present in the versions of Xen included in the firmware (e.g., CVE-2020-29568).

*Zlib*: CVEs present in the versions of zlib included in the firmware (e.g., CVE-2018-225032).

CVE Group	#CVEs	CVE Group	#CVEs
AMD CPU	3	Linux kernel	216
Android kernel	28	ncurses	7
ARM microprocessor	2	NETGEAR	2
Bluetooth	3	OpenSSH	8
BusyBox	16	OpenSSL	25
bzip2	2	Other	8
curl	35	PCRE (libpcre)	6
E2fsprogs	2	Shadow	3
expat (libexpat)	21	Wi-Fi	4
False positives	7	Windows 10 driver	2
glibc	34	Xen	2
Intel driver	2	zlib	2
Intel CPU	14		

#### Table 11: 454 Common CVEs by Group

## **Factors Affecting Study Repeatability**

There are two factors which may prevent this study from being repeatable. First, NIST continues to document new CVEs as they are identified by the cyber research community. The NVD added over 22,600 CVEs during the first 10 months of 2023 (NIST, 2023). The CSTs used in this study reference the NVD for CVE identification. Attempts to replicate this study by scanning firmware samples C1-C5 with the same CSTs and versions shown in Table 2 may result in additional CVEs being reported by the scans, due to the NVD containing CVEs which were added subsequent to the completion of this study. Secondly, each CST uses its own proprietary vulnerability detection algorithm. The CST vendors may change these algorithms over time. As a result, researchers attempting to replicate this study may notice differences in the CVEs identified in the CST scan reports *even if the contents of the NVD remained constant between replication attempts*.

## **Chapter Summary**

This chapter discussed the execution of the study. It described the process of obtaining the firmware samples, scanning them with CSTs, and examining the scan results. The study (as performed) varied significantly from its roadmap as described in Chapter 3. This chapter has attempted to explain why difficulties encountered in obtaining the sample population and access to CSTs required deviations from the original plan. The responsibility for those deviations, and the justifications provided in this chapter belong solely to the author.

## **CHAPTER 5: CONCLUSIONS**

### **Analysis of Objective**

The objective of this study was to identify vulnerabilities in 5G femtocell firmware using static analysis tools. It intended to determine if commercial SAST tools could be used to detect vulnerabilities in 5G femtocell firmware. To achieve this purpose, five samples of 5G femtocell firmware were analyzed by four CSTs. Each firmware sample was uploaded to online versions of each CST "in the blind." That is, no information about the provenance, contents, or function of the firmware sample were presented to the CST tool vendors, to preclude any possible biasing of the tool scan results.

Two hypotheses were to be tested by this study.  $H_0$ , the hypothesis which states that there are no detectable vulnerabilities in 5G femtocell firmware samples, was to be disproven by the successful detection of at least one vulnerability in any of the samples. The hypothesis  $H_1$ , which states that a significant amount of 5G femtocell firmware contains vulnerabilities (and is therefore exploitable) would be supported (but not proved) by the CST scans successfully detecting vulnerabilities in multiple 5G femtocell firmware samples. From analysis of  $H_1$ , the study was to determine if there was a correlation between 5G device manufacturers and the presence of vulnerabilities (device manufacturer  $\rightarrow H_1$ ).

Four metrics ( $M_x$ ) were to be computed from the study results. The sample with the highest number of reported CVEs, the sample having the CVE with the highest confidence value, the manufacturer having the highest percentage of samples for which at least one CVE has been found, and the CVE with the highest number of occurrences across all firmware samples ( $M_1$ - $M_4$  respectively).

The deliverables for this study were the determination of truth values for hypotheses  $H_0$  and  $H_1$ , the computation of metrics  $M_1$ - $M_4$ , and a resolution of the question of whether CSTs could be used to detect vulnerabilities in 5G femtocell firmware. All deliverables were dependent upon the CST scan results, which in turn were dependent upon the particular set of CSTs and firmware samples available to the researcher.

## **Findings**

### Determination of Truth Values for H<sub>0</sub> and H<sub>1</sub>

The null hypothesis  $H_0$  proposed that there were no vulnerabilities in 5G femtocell firmware which would be detectable by SAST tools. The CST scan results showed that multiple vulnerabilities were detected in *each* sample (C1-C5). While this data presents counterexamples to  $H_0$ , the confidence ratings of the detected vulnerabilities must also be considered before  $H_0$  can be considered disproven. In particular, the possibility that all detected vulnerabilities are false positives must be considered.

As shown in Chapter 4 (Table 9) three of the five firmware samples (C1, C3, C4) had at least one reported vulnerability with a confidence rating of C = 1.0. Multiple vulnerabilities were reported by the scans of C2 and C5, but neither sample contained a vulnerability which could be assigned a confidence value of 1.0. That was because some of the CSTs in *S* failed to complete their scans of those samples. These CST scan failures are identified on the C2 and C5 tabs of the *statistics.xlsx*, available to the Committee at a URL provided by DSU. The causes for these scan failures were due to errors in the tools themselves (scan crashed or entered an infinite loop) or by the size of the sample exceeding the maximum supported by the tool (sample C5 was 7.8GB when unzipped). Because the scan data for samples C2 and C5 is incomplete, this study cannot rule out the possibility that all reported vulnerabilities for those two samples were in fact false positives. For the other three samples in the study population, the confidence rating of C = 1.0 reduces the probability of *all* the reported vulnerabilities in those samples being false positives to  $\epsilon$  (a small nonzero value).

Hypotheses  $H_1$  postulated that a significant amount of 5G femtocell firmware contains vulnerabilities. As previously noted, the CST scans identified multiple vulnerabilities in all samples. These results provide supporting evidence for  $H_1$  but are insufficient for proof. The confidence in this supporting evidence is diminished by incomplete scan data for the C2 and C5 samples.

This study was unable to determine a correlation between 5G device manufacturers and the presence of vulnerabilities. This was due to the number of firmware samples (5) being less than the minimum number needed for statistical significance (16) and that only two manufacturers (ZTE and Ericsson) were represented in the study population.

### Set of Reported Vulnerabilities Varies by Tool

For each firmware sample, the set of reported vulnerabilities varied by tool. While a subset of the vulnerabilities in a particular sample were reported by more than one tool, this subset was *always* considerably smaller than the number of vulnerabilities for that sample reported by only one CST (Table 12). The low confidence rating (C = 0.25) assigned to the vulnerabilities reported only by a single CST suggests that they may be false positives.

Sample	Number of CVEs	Number of CVEs	Ratio of CVEs
	<b>Reported by Multiple</b>	Reported by a Single	<b>Reported</b> (Multiple
	CSTs ( <i>C</i> > 0.25)	<b>CST</b> ( $C = 0.25$ )	CSTs / Single CST)
C1	744	2780	0.2676
C2	660	1729	0.3817
C3	779	2580	0.3019
C4	873	2257	0.3868
C5	421	954	0.4413

Table 12: Ratio of CVEs Reported by Multiple CSTs / Single CST

#### **Report Terminology May Increase False Positives**

The terminology used for reporting vulnerabilities varied between CSTs. This could sometimes lead to benign information being classified as findings. For example, all CSTs classified passwords found in the firmware as "information leaks". Upon further investigation, it appears that the CST algorithms could not distinguish between plain text passwords and encrypted passwords. Reporting encrypted passwords as findings is misleading.

Another area where report terminology was not consistent across all CSTs was found in classifying the CVEs by severity. Severity classification terminology (Critical, High, Medium, Low, None/Unknown) is not necessarily interchangeable between different CSTs. While the classification algorithms were not made available for this study, it appears that the NIST CVSS score is used to determine CVE severity. However, care must be taken when reviewing the resulting severity classifications to verify which CVSS score (CVSS 2.0 or 3.0) was used by the CST creating the scan report. Some CSTs explicitly identify the CVSS version used, but others do not.

#### **CST Sample Size Limitations**

Some CSTs cannot scan samples larger than a certain size. The firmware samples used in this study varied in size from 455MB to 7.6GB (see Table 6). While all five CSTs in *S* were able to process the smaller samples, two CSTs failed to process the 7.6GB sample. Of those, one has a published maximum sample size limit of 7.0GB, the other has no such published maximum (it simply crashed during the scan).

CST ability to effectively scan firmware samples is also limited by the duration of the sample upload process. The scans for this study were performed by the online (i.e. "cloud") versions of the CSTs. This was necessary due to the researcher's computing resource constraints (absence of servers to run the CSTs locally) and constraints on the tools themselves (one of the CSTs only offers a cloud version). These CSTs require the firmware samples to be uploaded for analysis. The scans are performed in the cloud, with the scan reports available for subsequent download. Unlike the maximum sample size, which is determined by the size of the firmware sample, CST upload limitations are determined by the amount of time it takes for the upload to complete. For example, one of the CSTs terminated the upload process (without presenting an error message) after 30 minutes had expired, regardless of the amount of data uploaded. The firmware samples used for this study were uploaded using a consumer-grade residential broadband connection, which had insufficient speed to complete the upload within the required time limit. Therefore, each sample was zipped prior to uploading. The upload of each zipped sample was completed successfully. However, the zipped file sizes of the small number of samples available for study cannot encompass the entire range of zipped file sizes for all 5G femtocell firmware. Other firmware samples may be larger, and upload times longer. These factors may limit the utility of the cloud versions of certain CSTs.

#### **Each Firmware Sample Contained Multiple Vulnerabilities**

Each sample contained multiple unique CVEs (see Table 7). While the potential for false positives exists, the probability that *all reported CVEs are false positives is very low* (especially for those CVEs reported with  $C \ge 0.75$ ). This indicates that an attacker who gains access to one of the femtocells included in this study should be presented with multiple possible exploits.

### **Commercial SAST Tools Are "Works in Progress"**

All CSTs used in this study were commercially available during the summer of 2023. Their capabilities continue to be updated with new releases. One CST vendor is using their scan failures on samples C2 and C5 to improve their product and increase their maximum supported sample size. The vendor anticipates fixes for those failed scans to be included in the next release of their product (Alvino, 2023).

Eash CST uses its own proprietary algorithm for detection of CVEs. As previously seen, these algorithms differ in the set of CVEs detected on a given sample. Further, at least one vendor (Finite State) continued to modify their vulnerability detection algorithm while this study was being conducted. To illustrate the impact of algorithmic changes, consider Figure 155 and Figure 156 (Appendix H). Figure 155 shows scan results for sample C2 (submitted for analysis under the label "Sample 6"). Figure 156 shows scan results for sample C2 (submitted for analysis under the label "Sample C2"). The scan in Figure 155 was performed prior to the algorithm modification. The scan in Figure 156 was performed after the algorithm changes had been implemented. Note that the dates which appear in the figures (September 1, 2023, and August 31, 2023) are the dates that the reports were downloaded, not the dates that the scans were performed (the scan dates were June 16, 2023, and August 31, 2023, respectively).

From these two figures, it is evident that the vulnerabilities reported by a CST may differ, depending upon the particular algorithm in use at the time that the scan was performed. In the instance described above, Finite State stated that their algorithm was modified to reduce the number of false positives being reported, as shown in Figure 13 (in the "Emily" chat box). Regarding the scans of sample C2, the number of vulnerabilities reported actually *increased* from 3,492 to 10,207 after the algorithmic changes were implemented, so whether this objective was achieved remains an open question.

C3 TEST		< Emily	<u>≁</u>		
C2 TEST					
C1 TEST		<b>Active 45m ago</b> Oak Park, US			
	ſ	We have done some maintenance to how we handle some findings and wanted you to be aware that you will likely see reductions in your artifact finding counts and scores (in some cases, significant decreases!).			
VERSIONS	DEPE PRC				
1		of false positives for many customers. We're going to rework how we handle these and add them back in during the next few months - impacted customers will be alerted at that time of			
1		any additional changes to the finding counts. Our risk score decreases are due to the finding decreases combined with refreshed vulnerability data that is more accurately adjusted for exploitability potential (we use EPSS as part of			
1		this calculation in our risk scoring). More detailed information on how we approach scoring can be found in our <u>Help Center</u> .			
1		Write a reply If I are a reply	0		

Figure 13: Finite State Algorithm Changed to Reduce False Positives.

## Some 5G Firmware Deployed with Known CVEs

All firmware samples used in this study were harvested from 5G hardware which had been deployed in the field during 2020-2022. The CST scans reported CVEs which were dated between 1999 and 2023. These CVEs fall into two categories, those which were documented by NIST prior to removal of the 5G hardware from the field (e.g., CVE-2014-8502, detected in sample C1) and those documented only after the hardware had been removed from the field (e.g., CVE-2023-3220, detected in sample C1). The CVEs in the latter group might reasonably be expected to be detected, as they had not yet been identified in public CVE databases prior to the removal of the hardware devices from service. However, the presence of CVEs in the former group implies that the firmware was initially deployed containing CVEs already known to the cybersecurity community. It also indicates that those CVEs had not been mitigated by patches applied while the hardware was in service.

### Metric M<sub>1</sub>: Sample with the Highest Number of Unique CVEs

Each of the five samples had over 1300 unique CVEs detected by the CST scans. Sample C3 had the highest number of unique CVEs detected at 3759. Of those, five had a confidence rating of C = 1.0.

#### Metric M<sub>2</sub>: Sample with the Highest Number of Unique CVEs having C = 1.0

The CST scans detected unique CVEs with confidence ratings of C = 1.0 in only three of the five samples (C1, C3, C4). The absence of detected unique CVEs with C = 1.0 in the other two samples (C2, C5) should not be taken as evidence that none exist in those samples. Samples C2 and C5 were *exactly those samples for which one or more of the CST scans failed*. Had all CST scans of those samples been completed successfully, one or more unique CVEs with confidence ratings of C = 1.0 may have been detected in each sample.

#### Metric M<sub>3</sub>: 5G Manufacturer's Firmware Most Likely to Contain CVEs

No meaningful value could be computed for  $M_3$ , as the sample population was limited to four ZTE samples and one Ericsson sample. The CST scans identified 1377 unique CVEs in the Ericsson sample, while the average number of unique CVEs in the ZTE samples was 3200.5 (see Table 7). Interestingly, the average number of unique CVEs detected in the ZTE samples (C1-C4) with a confidence rating of C = 1.0 was 3. The number of unique CVEs detected in the Ericsson sample (C5) with a confidence rating of C = 1.0 was zero.

#### **Metric M4: The Unique CVE Most Commonly Detected in the Sample Population**

There was no single unique CVE which was most commonly found in the sample population. Rather, a set of 454 unique CVEs were detected in each of the five samples. The list of these unique CVEs is presented in Appendix A. Note that several of these CVEs (the 2009 through 2018 CVEs) were known to the cybersecurity community prior to the 5G firmware being deployed in the field.

## Assessment of Significance of the Findings

#### Vulnerabilities are Present in 5G Femtocell Firmware, and Detectable by SAST Tools

The study results are sufficient to disprove  $H_0$  and are supporting evidence for  $H_1$ . At a minimum, the CSTs used in this study are capable of detecting vulnerabilities in 5G femtocell firmware from multiple manufacturers. These CSTs could be employed by offensive cyber researchers wishing to compromise 5G femtocells from ZTE and Ericsson. The study results do not preclude these CSTs from being used to identify vulnerabilities in 5G femtocell firmware from other manufacturers. However, this study has shown vulnerability detection only on ZTE and Ericsson firmware.

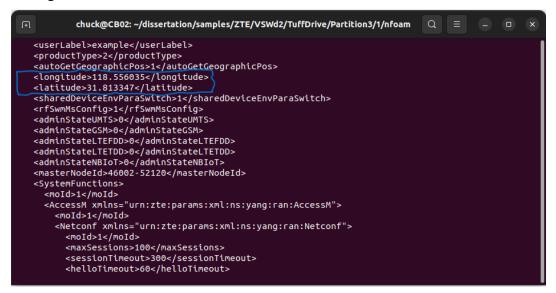
#### **Reported Vulnerabilities Vary by CST**

For each firmware sample, each CST reported a different set of vulnerabilities. While there was some overlap between the members of each set (i.e., those CVEs with C > 0.25) most vulnerabilities were reported by only one CST (see Table 10). One implication for cyber researchers is that the *failure* of any particular CST to detect a given CVE in a firmware sample is not sufficient evidence to prove that that CVE *is not present* in the sample. Another is that the *successful detection* of a given CVE in a firmware sample by any particular CST is insufficient evidence to prove that that CVE *is present* in the sample, due to the potential for false positives.

#### **Reported Information Leaks Might be False Positives**

Offensive security researchers may be interested in leveraging information leaked from the firmware (such as plaintext passwords, IP addresses, email addresses, etc.) to design attacks upon it. Care must be taken when using the "information leaks" reported by CSTs, as some of these were not true information leaks, and may lead an offensive security researcher into wasting time and resources attempting to exploit them. While the CSTs in this study did report some information leaks of interest (such as IP addresses and email addresses), others (e.g., the encrypted passwords noted earlier) do not supply exploitable information.

In certain cases, the CST algorithms missed detection of leaked information which may be of interest from an offensive perspective. For example, examination of a configuration file found in one of the ZTE samples revealed the geocoordinates of where the unit had been installed. This information was located without reference to the CST scan results. Rather, it was discovered by manually walking the firmware's directory tree and using the Linux utility *grep*. The leaked location information is shown in Figure 14, with the corresponding location mapped in Figure 15.





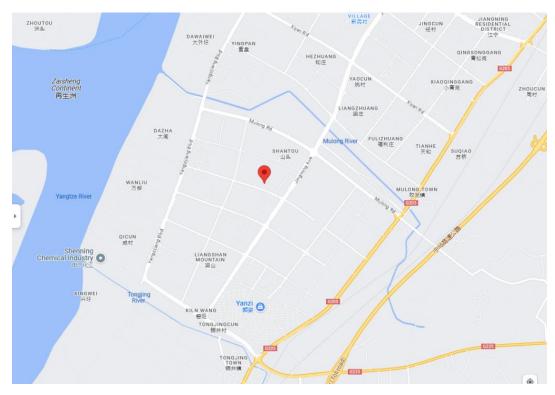


Figure 15: Corresponding Location of ZTE VSWd2 BBU, SW of Nanjing, China.

### **CST Limitations**

Although all the CSTs used in this study were cloud-based applications, the previously noted maximum supported sample size is a limiting factor. It is possible that other 5G femtocell firmware samples may be larger than those tested in this study. Such samples might exceed the maximum supported sample sizes of some CSTs, and therefore not be scannable by them. Security researchers must ensure that the uncompressed size of their firmware sample does not exceed the maximum for the tool to be used for scanning. Three of the four CSTs used in this study are also available in "on-premises" versions. The fourth tool vendor (Finite State) anticipates offering an on-premises version in the autumn of 2023. These locally hosted versions may lessen the impact of the upload time limits, while also making the tools accessible from inside air-gapped environments.

Certain CST vendors have chosen to limit the duration of the firmware sample upload process. This may limit the utility of those tools in areas with slow Internet upload speeds. While compressing a firmware sample prior to upload will reduce the upload time, even that tactic may be insufficient for very large firmware samples. In that case, it is advisable to split the sample into multiple sub-samples (if possible). The question of whether the combined scan results for the resulting sub-samples would be equivalent to those generated by scanning the sample as a single monolithic entity was beyond the scope of this study.

#### **5G Firmware May be Exploitable**

The number of CVEs identified by the CST scans coupled with their confidence ratings imply that the device firmware may be exploitable by offensive researchers. Physical access to the devices would not be required. If they can be attacked via the air interface, the attacker will be presented with a rich landscape of known CVEs which can be exploited. Even if we view the confidence ratings conservatively, considering only those firmware samples with C = 1.0 to be exploitable, three of the five samples tested meet this criterion (all are ZTE samples).

#### Scan Results May Not be Repeatable

Scanning a given firmware sample multiple times with the same CST may not yield identical results for each run. The reasons for this are twofold. First, new CVEs are constantly

being identified by the research community. Thus, repeating a firmware scan at a later date may detect new CVEs which were documented since the previous scan. Second, the CST vendor may have modified the CVE detection algorithm during the period between the scans (as seen with the Finite State Platform in Figures 151-153). The validity of scan results is therefore dependent upon the date that the scan was performed, and the CST version used. The possibility exists that false negatives from earlier scans may be reported as CVEs in later scans of the same firmware sample.

### Latent Vulnerabilities Exist in Fielded 5G Femtocells

The detection of known CVEs which predate deployment of the firmware samples implies that (for ZTE at least) 5G firmware is being installed in the field with known vulnerabilities. Whether this is being done intentionally or merely out of negligence is beyond the scope of this study. Regardless of the cause, the result is that some deployed 5G femtocells contain vulnerabilities that could be exploited.

#### **Correlation of Manufacturer to Presence of CVEs**

With only two 5G manufacturers in the sample population, efforts to determine a correlation between 5G device manufacturer and the presence of vulnerabilities were inconclusive. Although the average number of CVEs found in the four ZTE samples was higher than that found in the single Ericsson sample, that is insufficient evidence to conclude that 5G femtocell firmware from ZTE was more likely to contain vulnerabilities than that provided by Ericsson.

#### Significance of Metrics M<sub>1</sub>-M<sub>4</sub>

Of the five firmware samples in the study population, sample C3 (ZTE VSWd2 BBU controller board) had the highest number of unique CVEs detected ( $M_1$ ). Offensive cyber researchers seeking a "target rich environment" for the design of exploits should direct their efforts to this firmware. Sample C1 had the highest number of CVEs with a confidence rating of C = 1.0 ( $M_2$ ). Researchers interested in building exploits for the firmware sample which is most likely to contain true positive CVEs should target sample C1. Sample C3 may also be considered as a research target, as its number of CVEs with a confidence rating of C = 1.0 (five such CVEs) was only one less than that of sample C1 (six CVEs). The small size of the

study population precluded obtainment of a meaningful value for  $M_3$ . Therefore, that part of the research objective was not achieved.

Of the 14,180 CVEs detected in the study population, 4,658 were unique. Of those unique CVEs, 454 were detected in every member of the population (see Table 11). Offensive researchers interested in exploiting vulnerabilities most commonly found in the firmware under study should target the CVEs listed in Table 11. The remaining 4,204 unique CVEs all have confidence ratings of C < 1.0, indicating a higher probability of their being false positives.

## **Areas for Further Study**

The outcomes of this study present several possible avenues for further research. The 5G network continues to be deployed worldwide. 5G femtocells have begun to be deployed, but many more will need to be fielded to realize the promise of ubiquitous indoor 5G signal coverage. As new 5G femtocells enter the marketplace, they could form the sample population for a new study. The population for the current study was limited by the availability of firmware samples. Researchers able to directly contact major 5G infrastructure providers (such as Huawei) might be able to obtain a wider variety of firmware samples, enabling them to increase the study population size to the minimum needed for statistical significance (16 samples) and beyond.

Another research recommendation concerns the tools chosen for set *S*. The confidence ratings for this study were limited by the fact that the number of CSTs in *S* was small (T = 4). As noted in Chapter 1, the size of the error factor ( $\epsilon$ ) varies inversely with *T*. Executing this study with more tools in set *S* would increase the quality of the confidence ratings and decrease the possibility of reporting CVEs which were false positives. One way to increase the size of *S* would be to extend its membership beyond CSTs to include open-source SAST tools. The opportunity to compare the scan results from CSTs and open-source scans of the same firmware samples may offer another avenue of investigation.

Finally, the set of 454 common CVEs listed in Table 11 present questions for future researchers. Why were these CVEs seen across *all* samples, given that the samples came from two different manufacturers? Are there common libraries or operating system files that are used across multiple manufacturers' 5G femtocell products? If so, would an exploit created to

leverage one of these CVEs be successful against multiple manufacturers' 5G femtocell firmware? Taking this to an extreme, is it possible for an offensive researcher to build an exploit that would be effective against the 5G femtocell firmware of all manufacturers?

## **Summary**

This study showed that CSTs could be used successfully to detect vulnerabilities in 5G femtocell firmware. The set of reported CVEs is dependent upon the CST which performs the scan, and the version of that tool, as the underlying CVE detection algorithms are subject to change over time. Divergence of reported CVEs between CSTs scanning the same firmware sample is more common than convergence. Of the 4658 unique CVEs identified by the CSTs in this study, only 454 (9.75%) were identified by every tool. Of the 14180 CVEs reported in the scans of the study population, 10300 (72.64%) were identified by only one CST (which may indicate that they are false positives). The study faced obstacles in obtaining the desired firmware samples, due to import restrictions and the inability (or unwillingness?) of certain 5G femtocell vendors to support cyber research on their products. These limitations were partially overcome by obtaining used 5G hardware which had already been loaded with the desired firmware.

The study results show that certain 5G femtocell firmware contains known CVEs when first deployed. While such vulnerabilities might be expected to be removed by subsequent firmware updates, the study uncovered no evidence of such vulnerability mitigation. Whether this was due to a failure to apply firmware patches after product installation, or manufacturer decisions not to mitigate these vulnerabilities could not be determined.

The study found that there is little consensus on CVE detection between CSTs. The scan results were divergent, which lessens confidence in the accuracy of the CVE reports. The observation that 72.64% of CVEs found in the scan reports were reported by one CST but not the others, means that the tools in this study reported several false positives or that three of the four tools reported false negatives. Regardless of the cause, this performance should be of concern to the tool vendors, and a reminder to the cyber research community to be cautious in interpreting CST scan results.

This study contributes to the body of knowledge in the field of offensive cybersecurity by determining that the firmware of certain 5G femtocell products contains vulnerabilities which are detectable by CSTs. These results should serve as a call for 5G telecommunication infrastructure providers to improve the cybersecurity of their firmware, and as a caution to entities responsible for the deployment and cybersecurity of 5G networks. For offensive cyber researchers, the study results indicate the utility of CSTs for identifying vulnerabilities in 5G femtocell firmware.

## REFERENCES

- 3GPP. (2014a). 3GPP TR 21.908 Release 8 Description. In. Valbonne, France.
- 3GPP. (2014b). 3GPP TR 21.909 Release 9 Description. In. Valbonne, France.
- 3GPP. (2021). 3GPP TR 21.916 Release 16 Description. In. Valbonne, France.
- 3GPP. (2023). 3GPP TR 21.917 V17.0.1 Release 17. In. Valbonne, France: 3GPP.
- 5G Americas. (2019). The Evolution of Securty in 5G, A "Slice" of Mobile Threats. In.
- John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. Public Law 115-232 (2018).
- Secure 5G and Beyond Act of 2020, Government Printing Office, Pub. L. No. Public Law 116-129 (2020).
- ACM. (2020). Artifact Review and Badging Version 1.1. Retrieved from https://www.acm.org/publications/policies/artifact-review-and-badging-current
- Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials*, 21(4), 3682-3722. doi:10.1109/COMST.2019.2916180
- Alvino, V. (2023, September 14). [Code Sentry Evaluation follow-up meeting].
- AT&T. (2019, 2019-11-21). Tyndall Air Force Base to Use AT&T 5G Services. Retrieved from <u>https://about.att.com/story/2019/tyndall\_air\_force\_base.html</u>
- Babbie, R. (2020). The Practice of Social Research: Cengage Learning.
- Bhardwaj, A. (2020). 5G for Military Communications. *Procedia Computer Science*, 171, 2665-2674. doi:10.1016/j.procs.2020.04.289
- Biden, J. (2021). *Executive Order on Improving the Nation's Cybersecurity*. Washington: Washington: Federal Information & News Dispatch, LLC
- Blackberry. (2023). Blackberry Jarvis. Retrieved from https://blackberry.gnx.com/en/products/security/blackberry-jarvis
- Brake, D. (2020). A U.S. National Strategy for 5G and Future Wireless Innovation. In.
- Center for a New American Security. (2020). *Open Future The Way Forward on 5G*. Retrieved from
- CISA. (2020). CISA 5G Strategy.
- CISA. (2020b, October 21,2020). Critical Infrastructure Sectors. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors
- Cisco. (2020). *Cisco Vision: 5G THRIVING INDOORS*. Retrieved from <u>https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/ultra-</u> <u>services-platform/5g-ran-indoor.pdf</u>
- Crabtree, C., & Kern, H. L. (2018). Using Electromagnetic Signal Propagation Models for Radio and Television Broadcasts: An Introduction. *Political Analysis*, 26(3), 348-355. doi:10.1017/pan.2018.8
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.
- Defense Science Board. (2019). Defense Applications of 5G Network Technology.
- DePerry, D., Ritter, T., & Rahimi, A. (2013). Traffic interception and remote mobile phone cloning with a compromised CDMA femtocell. *DEF CON*.
- Desmaris, N. (2023, January 26). [RE: SCMS Enquiry Case # 00041894].
- Dhanasekaran, R. M. N., Suresh. (2023). *A comparison of 4G and 5G authentication methods* (CID210846 (February)). Retrieved from <u>https://onestore.nokia.com/asset/210846</u>

- DoD. (2020). DOD 5G Strategy Implementation Plan.
- DoD. (2020a). DOD Announces \$600 Million for 5G Experimentation and Testing at Five Installations [Press release]. Retrieved from <u>https://www.defense.gov/Newsroom/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati/</u>
- Eagle, C., & Nance, K. (2020). The Ghidra Book (1st edition ed.): No Starch Press.
- Edris, E. K. K., Aiash, M., & Loo, J. (2022). Formalization and evaluation of EAP-AKA' protocol for 5G network access security. *Array*, 16, 100254. doi:10.1016/j.array.2022.100254
- Ericsson. (2021a). 5G Cases. Retrieved from https://www.ericsson.com/en/5g/use-cases
- Ericsson. (2021b). Planning in-building coverage for 5G: from rules of thumb to statistics and AI, Extract from the Ericsson Mobility Report. Retrieved from <u>https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/indoor-outdoor</u>
- Ernest, W. B., Geraldine, T.-S., & Viktor, W. (2015). Survey Research: Methods, Issues, and the Future. In W. Viktor (Ed.), *Handbook of Research on Scholarly Publishing and Research Methods* (pp. 396-414). Hershey, PA, USA: IGI Global.
- ESF 5G Threat Model Working Panel. (2021). POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE. In: CISA.
- Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G\*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, 41(4), 1149-1160. doi:10.3758/BRM.41.4.1149
- FCC. (2020a). Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation ZTE Designation. In (Vol. 85, pp. 230). Washington: Washington: Federal Information & News Dispatch, LLC.
- In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation, (2020b).
- FCC. (2023). Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program. (2022-28263). Washington: US Government Printing Office Retrieved from <u>https://www.federalregister.gov/d/2022-28263</u>
- Finite State. (2019a). Finite State Supply Chain Assessment. Retrieved from

Finite State. (2019b). Finite State Responds to Huawei. Retrieved from <u>https://finitestate.io/blog/finite-state-responds-to-Huawei-Critiques-stands-by-assessment-huawei-products-contain-significant-vulnerabilities</u>

- Finite State. (2021). The Finite State Platform Automated Product Security for Connected Devices. In.
- Finite State. (2022). Manage risk across your software supply chain. Retrieved from <u>https://finitestate.io/products/finite-state-platform/</u>
- Fowler, F. J. (2014). Survey research methods (Fifth ed.).
- GAO. (2020a). GAO Tech Spotlight 5G Wireless. Retrieved from https://www.gao.gov/pdf/product/705363
- GAO. (2020b). Additional Actions Needed to Ensure Effectiveness of 5G Strategy. Retrieved from https://www.gao.gov/products/gao-21-155r

- Goel, S., & Nussbaum, B. (2021). Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. *IEEE Open Journal of the Communications Society*, 2, 1082-1093. doi:10.1109/OJCOMS.2021.3074591
- Goertz, G., & Mahoney, J. (2012). A Tale of Two Cultures : Qualitative and Quantitative Research in the Social Sciences. Princeton, N.J.: Princeton University Press.
- Grammatech. (2023). Code Sentry. Retrieved from <u>https://www.grammatech.com/our-products/codesentry/</u>
- GSMA Intelligence. (2020). *Mobile Economy 2020 North America*. Retrieved from Los Angeles: <u>https://www.gsma.com/mobileeconomy/northamerica/</u>
- Guthart, G. A. (2021). Low-Cost Unclassified Intelligence. Marine Corps Gazette.
- Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security Threats, Countermeasures, and Challenges of Digital Supply Chains. ACM Comput. Surv., 55(14s), Article 316. doi:10.1145/3588999
- HCSEC. (2019). HCSEC Oversight Board Report 2019. Retrieved from
- Hebei Shencheng, C. (2023). [Re: RE: To Charles Begian/Most popular-Huawei BBU 5900].
- Hou, J.-b., Li, T., & Chang, C. (2017). Research for vulnerability detection of embedded system firmware. *Procedia Computer Science*, 107, 814-818.
- Hu, X., Liu, C., Liu, S., You, W., Li, Y., & Zhao, Y. (2019). A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security. *IEEE Access*, 7, 125424-125441. doi:10.1109/ACCESS.2019.2937997
- Huawei. (2019a). Huawei Statement on Finite State. Retrieved from https://www.huawei.com/en/facts/voices-of-huawei/finite-state-letter
- Huawei PSIRT. (2019b). Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment. Retrieved from <u>https://www.huawei.com/en/psirt/security-notices/huawei-sn-20190702-01-finitestate-en</u>
- Jackson, F. E. (2002). *Tannenberg: The First Use of Signals Intelligence in Modern Warfare*. Retrieved from
- Ji, H., Park, S., Yeo, J., Kim, Y., Lee, J., & Shim, B. (2017). Introduction to Ultra Reliable and Low Latency Communications in 5G. *ArXiv*, *abs/1704.05565*.
- Joern.io. (2023). Joern the Bug Hunter's Workbench. Retrieved from https://joern.io/
- Jover, R. P., & Marojevic, V. (2019). Security and Protocol Exploit Analysis of the 5G Specifications. *IEEE Access*, 7, 24956-24963. doi:10.1109/ACCESS.2019.2899254
- Leleux, D., Woodruff, R., Perry, K., & Bergesen, D. (2021). Fifth Generation Wireless Development in Great Power Competition
- Department of Defense Implications and Policy Recommendations. *The Cyber Defense Review*, 6(1), 15-32. Retrieved from <u>https://www.jstor.org/stable/26994111</u>
- Lum, E. (2023). RF SMP Board-to-Board Connectors Market Review. *Microwave Journal*, 66(3), 86-88,90,92. Retrieved from <u>https://www.microwavejournal.com/articles/39786-rf-smp-board-to-board-connectors-market-review</u>
- Lumenci Team. (2021, October 28, 2021). 5G Beamforming. Retrieved from https://www.lumenci.com/research-articles/5g-beamforming
- Medin, M., & Louie, G. (2019). *The 5G ecosystem: Risks and opportunities for DoD*. Retrieved from
- MITRE Corporation. (2021). CVE. Retrieved from <u>https://www.cve.org/</u>

- Morrison, M. I. (2013). THE ACQUISITION SUPPLY CHAIN AND THE SECURITY OF GOVERNMENT INFORMATION TECHNOLOGY PURCHASES. *Public Contract Law Journal*, 42(4), 749-792. Retrieved from <u>https://www.jstor.org/stable/24430332</u>
- National Academies of Sciences, E., & Medicine. (2019). *Reproducibility and replicability in science*. Washington, District of Columbia: National Academies Press.
- Nebbia, C. B. (2010). Federal Spectrum Management at the National Telecommunications and Information Administration. In NTIA (Ed.): NTIA.
- NIST. (2021, December 15, 2021). Source Code Security Analyzers. Retrieved from https://www.nist.gov/itl/ssd/software-quality-group/source-code-security-analyzers
- NIST. (2022). *National Institute of Standards and Technology Special Publication 1800-33B*. Gaithersburg, MD Retrieved from <u>https://www.nccoe.nist.gov/5g-cybersecurity</u>
- NIST. (2023). National Vulnerability Database. Retrieved from <u>https://nvd.nist.gov/general/nvd-dashboard</u>
- Nokia. (2019). *Nokia AirScale System Module Product Description*. 5G RAN, Rel. 5G19, Operating Documentation, Pre-release, Issue 4. Technical Manual.
- NTIA. (2021). National Strategy to Secure 5G Implementation Plan and Annexes A F.
- Olimid, R. F., & Nencioni, G. (2020). 5G Network Slicing: A Security Overview. *IEEE Access*, 8, 99999-100009. doi:10.1109/access.2020.2997702
- Osibo, B. K., Zhang, C., Xia, C., Zhao, G., & Jin, Z. (2021). Security and Privacy in 5G Internet of Vehicles (IoV) Environment. *Journal on Internet of Things*, 3(2), 77-86. doi:10.32604/jiot.2021.017943
- Osterhage, W. (2018). *Wireless network security* (Second edition. ed.). Boca Raton, FL: CRC Press, an imprint of Taylor and Francis.
- Ostien, T. (2022, November 7). [Small Cell Inquiry].
- Otten, A. (2023). Cirriculum Vitae. Retrieved from

https://sites.google.com/site/aotteneport/curriculum-vitae

- Penttinen, J. T. J. (2019). 5G Explained: Security and Deployment of Advanced Mobile Communications. Newark: Newark: John Wiley & Sons, Incorporated.
- Prague 5G Security Conference. (2019). The Prague Proposals.
- Pruitt, K. L. (2020). 5G Threats and Opportunities. (M.S.). San Diego State University, San Diego. Retrieved from <u>https://digitallibrary.sdsu.edu/islandora/object/sdsu%3A59794</u> ProQuest Dissertations & Theses Global database. (28263188)
- Redini, N. (2020). Analyzing and Securing Firmware for IoT Devices. In: eScholarship, University of California.
- Repasi, R. (2023, February 17). [Letter of Repasi to Terrasi II].
- Rodriguez, J. (2015a). Small Cells for 5G Mobile Networks. In (1 ed., pp. 63-104). Chichester, UK: Wiley.
- Saldana, J. (2011). *Fundamentals of Qualitative Research*. New York: Oxford University Press.
- Sbisa, D. (2022, June 29). [Sorry For the Delayed Response].
- Secretary of Defense. (2020). Department of Defense (DoD) 5G Strategy

Sevastopulo, D., & Kerr, J. (2022). Canada to ban Chinese telecoms Huawei and ZTE from 5G networks. *FT.com*. Retrieved from <u>https://www.ft.com/content/2534ca85-b08e-4f78-88f3-c04770b41a02</u>

- Song, L., Xu, Z., Tian, Z., Chen, J., & Zhi, R. (2019). Research on 4G And 5G Authentication Signaling. *Journal of Physics: Conference Series*, 1213, 042048. doi:10.1088/1742-6596/1213/4/042048
- Sourceforge.io. (2023). CPPcheck. Retrieved from https://cppcheck.sourceforge.io/
- Stacey, K. (2019). Pentagon wants open-source 5G plan in campaign against Huawei. *FT.com*.
- Statista. (2016). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. Retrieved from <u>https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/</u>
- Stepanets, I., Fokin, G., & Müller, A. (2019). *Beamforming Techniques Performance Evaluation for 5G Massive MIMO Systems.* Paper presented at the CERC.
- Synopsys. (2023, 2023). Black Duck Binary Analysis. Retrieved from <u>https://www.synopsys.com/software-integrity/security-testing/software-composition-analysis/binary-analysis.html</u>
- T-Mobile USA. (2020). Un-carrier 5G Fact Sheet.
- Tannahill, G. (2023, January 27). [Your inquiry about Huawei and ZTE Equipment].
- Terrell, S. R. (2015). Writing a proposal for your dissertation: Guidelines and examples.
- Thompson, J. (2022, July 11). [Crown Castle and Dakota State University].
- Trump, D. J. (2018). National Cyber Strategy. Washington, D.C.
- Trump, D. J. (2019). Executive Order on Securing the Information and Communications Technology and Services Supply Chain. In. Washington: Washington: Federal Information & News Dispatch, LLC.
- Trump, D. J. (2020). National Strategy to Secure 5G.
- United States White House Office. (1990). NSD 42. Retrieved from <u>https://www.hsdl.org/?view&did=458706</u>
- Verizon. (2020). What are phone bands (GSM, CDMA) and why do they matter? Retrieved from <u>https://www.verizon.com/articles/Smartphones/what-are-phone-bands-and-why-do-they-matter/</u>
- Wieringa, R. J. (2014). Design science methodology for information systems and software engineering: Springer.
- Wyckhouse, M. (2022, January 11). [Re: Finite State Platform discussion].
- Yao, J., & Zimmer, V. (2020). Proactive Firmware Security Development. In J. Yao & V. Zimmer (Eds.), *Building Secure Firmware: Armoring the Foundation of the Platform* (pp. 17-63). Berkeley, CA: Apress.
- Zhang, S. (2019). An Overview of Network Slicing for 5G. *IEEE Wireless Communications*, 26(3), 111-117. doi:10.1109/mwc.2019.1800234
- ZTE. (2020). ZXRAN V9200 Product Description. Technical Manual. ZTE Corporation.

# **APPENDICES**

## **APPENDIX A: 454 COMMON VULNERABILITIES**

A set of 454 common vulnerabilities were identified in every firmware sample (C1-C5). These are presented in Table 13. Seven CVEs known to be false positives are indicated with an asterisk (\*).

CVE-2009-5155	CVE-2019-18805	CVE-2020-27066	CVE-2021-38604	CVE-2022-26490
CVE-2013-0340	CVE-2019-19126	CVE-2020-27068	CVE-2021-3864	CVE-2022-27666
CVE-2013-4235	CVE-2019-19252	CVE-2020-27618	CVE-2021-39537	CVE-2022-27774
CVE-2014-2524	CVE-2019-19319	CVE-2020-27675	CVE-2021-39633	CVE-2022-27776
CVE-2015-0569	CVE-2019-19527	CVE-2020-27777	CVE-2021-39634	CVE-2022-27781
CVE-2015-0570	CVE-2019-19537	CVE-2020-27780	CVE-2021-39686	CVE-2022-27782
CVE-2015-0571	CVE-2019-19767	CVE-2020-28097	CVE-2021-3995	CVE-2022-28321
CVE-2015-2877	CVE-2019-19768	CVE-2020-28974	CVE-2021-3996	CVE-2022-28356
CVE-2015-7312	CVE-2019-19769	CVE-2020-29368	CVE-2021-3998	CVE-2022-28391
CVE-2015-8553	CVE-2019-19770	CVE-2020-29370	CVE-2021-3999	CVE-2022-29458
CVE-2016-10228	CVE-2019-19814	CVE-2020-29373	CVE-2021-4002	CVE-2022-2961
CVE-2016-10739	CVE-2019-19922	CVE-2020-29562	CVE-2021-40439	CVE-2022-2978
CVE-2016-2853	CVE-2019-1999	CVE-2020-29568	CVE-2021-40490	CVE-2022-29900
CVE-2016-2854	CVE-2019-20054	CVE-2020-29573	CVE-2021-4083	CVE-2022-29901
CVE-2016-3189	CVE-2019-20096	CVE-2020-29660	CVE-2021-4157	CVE-2022-2991
CVE-2017-11164	CVE-2019-20794	CVE-2020-29661	CVE-2021-4160	CVE-2022-30065
CVE-2017-7244	CVE-2019-20795	CVE-2020-35501	CVE-2021-41617	CVE-2022-3028
CVE-2017-7246	CVE-2019-20812	CVE-2020-35508	CVE-2021-4197	CVE-2022-30594
CVE-2018-1000500	CVE-2019-20838	CVE-2020-36312	CVE-2021-4203	CVE-2022-32206
CVE-2018-12126	CVE-2019-2181	CVE-2020-36322	CVE-2021-4204	CVE-2022-32208
CVE-2018-12127	CVE-2019-2213	CVE-2020-36394	CVE-2021-42327	CVE-2022-32221
CVE-2018-12130	CVE-2019-25013	CVE-2020-36516	CVE-2021-42374	CVE-2022-32250
CVE-2018-12207	CVE-2019-3874	CVE-2020-36557	CVE-2021-42376	CVE-2022-3238
CVE-2018-16862	CVE-2019-5188	CVE-2020-36558	CVE-2021-42378	CVE-2022-32981
CVE-2018-18397	CVE-2019-5489	CVE-2020-4788	CVE-2021-42379	CVE-2022-33744
CVE-2018-19211	CVE-2019-5747	CVE-2020-6096	CVE-2021-42380	CVE-2022-3522*
CVE-2018-19217	CVE-2019-6109	CVE-2020-8177	CVE-2021-42381	CVE-2022-35252
CVE-2018-19591	CVE-2019-6488	CVE-2020-8231	CVE-2021-42382	CVE-2022-3534
CVE-2018-19824	CVE-2019-6974	CVE-2020-8284	CVE-2021-42384	CVE-2022-3643
CVE-2018-20679	CVE-2019-7308	CVE-2020-8285	CVE-2021-42385	CVE-2022-3715
CVE-2018-20685	CVE-2019-7309	CVE-2020-8286	CVE-2021-42386	CVE-2022-37434
	1	1	1	

Table 13: The 454 Unique CVEs Detected in Every Sample C1-C5

CVE-2018-20796	CVE-2019-8956	CVE-2020-8647	CVE-2021-43396	CVE-2022-39046
CVE-2018-20843	CVE-2019-9169	CVE-2020-8648	CVE-2021-45485	CVE-2022-39188
CVE-2018-25032	CVE-2019-9192	CVE-2020-8649	CVE-2021-45486	CVE-2022-39842
CVE-2018-5407	CVE-2019-9445	CVE-2020-8992	CVE-2021-45960	CVE-2022-40476
CVE-2018-7169	CVE-2019-9453	CVE-2021-0605	CVE-2021-46143	CVE-2022-40540
CVE-2018-9445	CVE-2019-9503	CVE-2021-0707	CVE-2022-0330	CVE-2022-40674
CVE-2019-0136	CVE-2019-9506	CVE-2021-0929	CVE-2022-0400	CVE-2022-42703
CVE-2019-0148	CVE-2020-0009	CVE-2021-1048	CVE-2022-0480	CVE-2022-4304
CVE-2019-0154	CVE-2020-0067	CVE-2021-20317	CVE-2022-0492	CVE-2022-43552
CVE-2019-1010022	CVE-2020-0427	CVE-2021-20320	CVE-2022-0494	CVE-2022-43680
CVE-2019-1010023	CVE-2020-0431	CVE-2021-20321	CVE-2022-0563	CVE-2022-43750
CVE-2019-1010024	CVE-2020-0432	CVE-2021-20322	CVE-2022-0778	CVE-2022-4450
CVE-2019-1010025	CVE-2020-0444	CVE-2021-22555	CVE-2022-0850	CVE-2022-4543
CVE-2019-10207	CVE-2020-0543	CVE-2021-22876	CVE-2022-0854	CVE-2022-45919
CVE-2019-10220	CVE-2020-10029	CVE-2021-22898	CVE-2022-1011	CVE-2022-4662
CVE-2019-10638	CVE-2020-10135	CVE-2021-22922	CVE-2022-1016	CVE-2022-48502
CVE-2019-10639	CVE-2020-10711	CVE-2021-22923	CVE-2022-1199	CVE-2023-0030
CVE-2019-11091	CVE-2020-10720	CVE-2021-22924	CVE-2022-1204	CVE-2023-0047*
CVE-2019-1125	CVE-2020-10751	CVE-2021-22925	CVE-2022-1205	CVE-2023-0215
CVE-2019-11477	CVE-2020-10766	CVE-2021-22926	CVE-2022-1247	CVE-2023-0266
CVE-2019-11478	CVE-2020-10767	CVE-2021-22946	CVE-2022-1271	CVE-2023-0286
CVE-2019-11479	CVE-2020-10768	CVE-2021-22947	CVE-2022-1292	CVE-2023-0394
CVE-2019-11486	CVE-2020-10773	CVE-2021-23840	CVE-2022-1304	CVE-2023-0458
CVE-2019-11487	CVE-2020-11565	CVE-2021-23841	CVE-2022-1353	CVE-2023-0464
CVE-2019-11599	CVE-2020-11669	CVE-2021-26341	CVE-2022-1508	CVE-2023-0465
CVE-2019-11833	CVE-2020-12062	CVE-2021-26401	CVE-2022-20141	CVE-2023-0466
CVE-2019-12381	CVE-2020-12114	CVE-2021-27645	CVE-2022-20148	CVE-2023-0687
CVE-2019-12614	CVE-2020-12464	CVE-2021-28660	CVE-2022-20158	CVE-2023-1206
CVE-2019-12615	CVE-2020-12656	CVE-2021-28831	CVE-2022-20166	CVE-2023-2007
CVE-2019-12819	CVE-2020-12770	CVE-2021-28951	CVE-2022-20424*	CVE-2023-2248*
CVE-2019-12900	CVE-2020-12826	CVE-2021-28972	CVE-2022-20566	CVE-2023-23916
CVE-2019-13272	CVE-2020-13143	CVE-2021-29265	CVE-2022-20568	CVE-2023-2513
CVE-2019-13648	CVE-2020-13974	CVE-2021-29650	CVE-2022-20572	CVE-2023-25139
CVE-2019-14615	CVE-2020-14145	CVE-2021-31829	CVE-2022-2068	CVE-2023-2602
CVE-2019-14821	CVE-2020-14155	CVE-2021-32078	CVE-2022-2097	CVE-2023-2603
CVE-2019-15117	CVE-2020-14314	CVE-2021-33033	CVE-2022-21123	CVE-2023-2650
CVE-2019-15118	CVE-2020-14331	CVE-2021-3326	CVE-2022-21125	CVE-2023-26545
CVE-2019-15212	CVE-2020-14351	CVE-2021-3347	CVE-2022-21166	CVE-2023-27533
CVE-2019-15214	CVE-2020-14381	CVE-2021-33574	CVE-2022-21385	CVE-2023-27534
CVE-2019-1543	CVE-2020-14386	CVE-2021-33656	CVE-2022-22576	CVE-2023-27535
CVE-2019-1547	CVE-2020-15436	CVE-2021-33909	CVE-2022-22822	CVE-2023-27536

CVE-2019-1551	CVE-2020-15437	CVE-2021-3428	CVE-2022-22823	CVE-2023-27538
CVE-2019-1552	CVE-2020-15778	CVE-2021-3449	CVE-2022-22824	CVE-2023-28319
CVE-2019-1563	CVE-2020-16120	CVE-2021-34556	CVE-2022-22825	CVE-2023-28320
CVE-2019-15666	CVE-2020-1749	CVE-2021-35477	CVE-2022-22826	CVE-2023-28321
CVE-2019-15903	CVE-2020-1751	CVE-2021-35942	CVE-2022-22827	CVE-2023-28322
CVE-2019-15916	CVE-2020-1752	CVE-2021-36368	CVE-2022-23218	CVE-2023-29383
CVE-2019-15927	CVE-2020-1971	CVE-2021-3655	CVE-2022-23219	CVE-2023-29491
CVE-2019-16905	CVE-2020-24586	CVE-2021-3711	CVE-2022-23816*	CVE-2023-32269
CVE-2019-16994	CVE-2020-24587	CVE-2021-3712	CVE-2022-23852	CVE-2023-34255*
CVE-2019-17052	CVE-2020-25211	CVE-2021-3714	CVE-2022-23960	CVE-2023-34256
CVE-2019-17055	CVE-2020-25212	CVE-2021-3732	CVE-2022-23990	CVE-2023-35001
CVE-2019-17075	CVE-2020-25285	CVE-2021-3753	CVE-2022-24448	CVE-2023-3640
CVE-2019-17133	CVE-2020-25656	CVE-2021-37576	CVE-2022-24958	CVE-2023-37453
CVE-2019-17351	CVE-2020-25704	CVE-2021-37600	CVE-2022-25235	CVE-2023-3772
CVE-2019-17594	CVE-2020-26140	CVE-2021-3772	CVE-2022-25236	CVE-2023-3817
CVE-2019-17595	CVE-2020-26141	CVE-2021-38160	CVE-2022-25265	CVE-2023-38408
CVE-2019-18276	CVE-2020-26144	CVE-2021-38205	CVE-2022-25313	CVE-2023-4010
CVE-2019-18282	CVE-2020-26145	CVE-2021-38300	CVE-2022-25314	CVE-2023-4205*
CVE-2019-18683	CVE-2020-26555	CVE-2021-3847	CVE-2022-25315	

# **APPENDIX B: E-MAIL CORESPONDENCE**

## E-mail messages pertinent to this study appear in Figure 16 through Figure 19.

Sbisa, Dan < Dan. Sbisa@commscope.com >	٢	← Reply	≪ Reply All	$\rightarrow$ Forward	<b>i</b>
<ul> <li>Source Dear Address Common Source Common Sour</li></ul>				Wed 6/29,	/2022 12:17 PN
Tou replied to this message on 0/29/2022 12:41 PM.					
i Charles, sorry for the delayed response. For clarification CommScope does not offer a femto product. Our OneCell p apacity of 1024 users. In addition, our OneCell product is only purchased by our certified partners or directly by the MM nrough these channels to ensure the Operators licensed 4G and 5G spectrum is deployed accordingly. Unfortunately,	IO. Our contractual agreement(s) with the	ne Operator(s	) require us to o	offer our small c	
iegards,					
Dan Sbisa Jusiness Development – Small Cells					
COMMSCOPE"					
now meets next					
13.284.9037					
Figure 16: CommScope Resp	onse (Sbisa, 2022)				
TJ Thompson, John <john.thompson@crowncastle.com></john.thompson@crowncastle.com>	٢	← Reply	≪ Reply All	→ Forward Mon 7/11/	(2022 11:20 AN
(1) You replied to this message on 7/11/2022 1:46 PM.					
You don't often get email from john.thompson@crowncastle.com. Learn why this is important					
- harles, We do not have these devices. Are you interested in improving the cell coverage on the campus or are you just doing	some research?				
ohn Thompson					
Director of Inside Sales T: (978) 266-9339   M: (603) 703-1880					
C <b>ROWN CASTLE</b> 1800 W Park Dr Westborough, MA 01581 www.crowncastle.com					
am looking for indoor 5G femtocell devices for university research. Does your firm offer such a device? If not, do you kn This email may contain confidential or privileged material. Use or disclosure of it by anyone other than the recipient is un			se delete this er	nail.	
Figure 17: Crown Castle Response (1	hompson, 2022)				
tim.ostien@accuver.com	١	← Reply	≪ Reply All	$\rightarrow$ Forward	<b>i</b>
To Begian, Charles Cc Cronin, Kyle				Mon 11/7	7/2022 10:23 AI
(i) You replied to this message on 11/7/2022 10:25 AM.					
Hi Chuck,					
My apologies for the delay in response. Unfortunately, I received word from our HQ that they are unable to sell just one small cell. We d certain MoQ with our factory.	on't have a stock here in the US and our HQ is	s focusing on la	arge scale opportu	inities based on m	neeting a

I'm sorry to deliver this news, but that is the directive that I received.

Thanks, Tim

Figure 18: Accuver Response (Ostien, 2022)

#### Your inquiry about Huawei and ZTE Equipment

CT	George
U	To Begiar

George Tannahill <George.Tannahill@fcc.gov> To Begian, Charles

Follow up. Start by Tuesday, August 15, 2023. Due by Tuesday, August 15, 2023. You forwarded this message on 1/27/2023 1:28 PM. You don't often get email from george.tannahill@fcc.gov. Learn why this is important

#### Hi Charles,

This is in response to our phone conversation today.

The FCC released FCC 22-84 on November 25, 2022 related to prohibiting equipment authorization of specific devices produced by entities identified on a covered list that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.

When the rules become effective upon publication in the Federal Register, FCC 22-84 will prohibit new equipment authorizations for specific equipment produced by entities named on the covered list. Huawei and ZTE are both entities named on the covered list.

FCC 22-84 prohibits the authorization of new equipment but doesn't prohibit the importation of equipment already approved.

The FCC database for approved equipment is available at: https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

Approved devices will have an FCCID on them. In the link above the FCCID is made up of a Grantee code (3 characters if it starts with a letter and 5 characters if it starts with a number) and a product code (1-14 additional characters) which can be entered in the appropriate fields above.

If you have additional questions they can be submitted to the FCC OET Knowledge Database at: <u>www.fcc.gov/kdb</u> using the link for submit an inquiry. Selecting the appropriate categories for covered equipment will get the question directly to someone who can respond.

With regard to your question on importation, the FCC importation rules are viewable at: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-2/subpart-K Specifically 2.1204.

Regards,

George Tannahill FCC Office Of Engineering and Technology Laboratory

Figure 19: FCC Clarification of Rule 22-84



Federal Communications Commission Washington, D.C. 20554

February 17, 2023

The Honorable Marco Rubio Attention: Martin J. Terrasi II 201 South Orange Avenue, Suite 350 Orlando, FL 32801

Dear Senator Rubio:

Thank you for your letter dated January 25, 2023, on behalf of your constituent, Mr. Charles Begian. On January 27, 2023, staff from the Office of Engineering and Technology reached out to Br. Begian to address his concerns and answer his questions.

Please let us know if we can be of further assistance.

Sincerely

Ronald T. Repasi Acting Chief Office of Engineering and Technology

Figure 20: Letter documenting FCC's quick response to inquiry on Rule 22-84

Re: RE: To Charles Begian/Most popular-Huawei BBU 5900

 $\bigcirc$  ← Reply ≪ Reply All → Forward 📑 ···· colin@hbscheng.com To Begian, Charles Mon 1/30/2023 8:49 PM Follow up. Start by Monday, February 6, 2023. Due by Monday, February 6, 2023. You replied to this message on 2/6/2023 3:54 PM. You don't often get email from colin@hbscheng.com. Learn why this is important Hello dear, Thanks for your reply. Thanks for your reply. Yes,we can split to some parts and send to you.In addition,change the brand name is also possible. What is your quantity?Do you only want the second hand? Waiting for your reply. From: <u>Begian, Charles</u> Date: 2023-01-31 00:16 To: <u>colin@hbkshena.com</u> Subject: RE: To Charles Begian/Most popular-Huawei BBU 5900 Colin, I don't think we will be able to import an entire BBU 5900 into the US due to import ban by the US FCC. At this point, we may only be able to purchase used BBU components. We are researching what components we need to buy. This is delayed as many Alibaba.com suppliers are on holiday for the New Year. We should get moving on this again next week. -Charles Begian From: colin@hbscheng.com <colin@hbscheng.com> Sent: Sunday, January 29, 2023 9:38 PM To: Begian, Charles <<u>Charles.Begian@trojans.dsu.edu</u>> Subject: To Charles Begian/Most popular-Huawei BBU 5900 You don't often get email from colin@hbscheng.com. Learn why this is important Hi Charles Begian, Glad to learn you're on the market of Huawei BBU 5900 products. We have many years experience on this field,can provide the best products and the lowest rate to maximize profits. If you are interested in please contact me. Best regards, Colin Foreign trade manager Hebei Shencheng Trading Co ltd Add:No 168,Jiantong Street,Yuhua District,Shijiazhuang City,Hebei Province,China Web:www.hbscheng.com **SH** 

Figure 21: Offer to "white label" a Huawei BBU

# **APPENDIX C: CST SCAN REPORT EXCERPTS FOR SAMPLE C1**

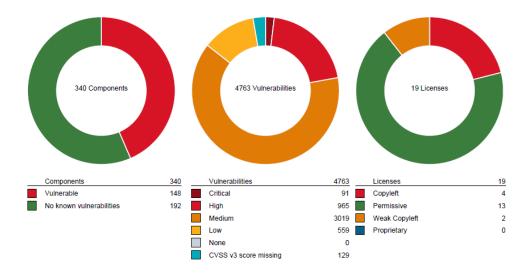
#### Black Duck Binary Analysis Search and jump to group. 🕹 Upload 🛛 👻 은 charles.begian sample\_C1.zip Vulnerability analysis Information leakage Executable attributes Static code analysis Feed Analysis settings File content General Name sample\_C1.zip 🕑 Description No description given 🗹 Version No version given 🗹 Uploaded 2023-08-10 00:14 (5 days ago) by charles.begian Last scanned 2023-08-10 01:08 (5 days ago) 20230608 BDBA engine version used for scanning 20230615 LATEST BDBA frontend version used for calculation Protect from data retention Notify on new vulnerabilities **File properties** File A Replace File available No SHA1 0330fa2c3f3e0e83e87ccd97255a855497892060 Size 3.66 GB (original) / 14.85 GB (scanned) Analysis © Remove Application type ELF binary Duration an hour Throughput ③ 68.73 MB/s BDSA database version ③ 2023-08-14T11:59:50 STALE NVD database version ③ 2023-08-14T06:15:00 STALE 2023-08-14T04:04:31 Component database version ③ Native fingerprint version 2023-05-31T10:04:47 Dotnet fingerprint version 2023-05-31T04:12:23.653096 2023-06-07T07:52:47.754010 Cocoapods fingerprint version Golang fingerprint version 2023-06-08T07:16:22.448950

# Sample C1 Black Duck Scan Report Excerpts

Figure 22: C1 Scan Overview (Black Duck)

## sample\_C1.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY





Report generated 2023-08-13T22:21:10Z https://protecode-sc.com/products/24698186

### Details

Original filename	
SHA1 checksum	0330fa2c3f3e0e83e87ccd97255a855497892060
Original file size	3661.65 MB

#### Infoleak

Asymmetric keys:	725
AWS keys:	0
Custom pattern matches:	0
Emails:	12945
HTTP authentication:	0
Image metadata:	0
IP addresses:	9597
JSON web tokens:	0
MAC addresses:	152
OAuth tokens:	0
Passwords:	387
Shell history:	6
URLs:	6555
Twilio keys:	0
Google cloud keys:	0
Facebook access tokens:	0

Figure 24: C1 Information leaks (Black Duck)

0 PEM         TRUE         TRUE         Image         ["sample_C1.zip", WMe/sol/Livesion/VEN/V2.10.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.317667662           05A         1004 PEM         TRUE         FALSE         ["sample_C1.zip", WMe/sol/Livesion/VEN/V2.10.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_2020002519125.osg/1v2.210.00899-3902-14_2020002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.210.00899-3902-14_202002519125.osg/1v2.100.0089-3902-14_2020025191	Algorithm E	Bits Format	Private	Encrypted Co	ontent User	Expires	CertificatxAttributesFile
DSA         1004 PEM         TRUE         FALSE		0 PEM	TRUE	TRUE '			['sample_C1.zip', 'W/Me/registry/docker/docker/negistry/v2/blobs/sha256/cr/cx944d37e3318f5b783e9e520d22a79fe784b04d14f9d72d09eeed25a58133cd/data', 'version/liib/librosng.so"]
RSA         2048 PEM         TRUE         FALSE         Image: Clarpity: WMe/docker/overlag/Deb8021264F3502135484993984F778aab/18do6a4f8544111e8021e32/diffsf501/brat; rss. [rev]           DSA         1004 PEM         TRUE         FALSE         Image: Clarpity: WMe/docker/overlag/Deb8021264F3502135484993984F778aab/18do6a4f8544411e8021e32/diffsf50213548420358027876e34430F33185677828452035022778E784540418572039ee425550322           0 PEM         TRUE         TRUE         Image: Clarpity: WMe/docker/overlag/Deb8021270483702100845_g43420550322778/F8454043185731856778284520022778E784540418572039ee425550322           0 PEM         TRUE         Image: Clarpity: WMe/docker/overlag/Deb905472078ee42504237678/F845404318572039ee42550322           0 PEM         TRUE         Image: Clarpity: WMe/docker/overlag/Deb905485535302         PME/docker/overlag/Deb90544320503023778/F845404005010447142402005313253.pdf-128-766966           RSA         2048 PEM         TRUE         FALSE         Image: Clarpity: WMe/docker/overlag/Deb9054565573655661ab0cff4bab0150184e4715448ab06000/dff1home/levenmt/config/beega/s           RSA         2048 PEM         TRUE         FALSE         Image: Clarpity: WMe/docker/overlag/Deb939024_4_202003513232.webmt; 72.20.10089-29024_4_202003519323.webmt; 72.20.10089-2		0 PEM	TRUE	TRUE '			['sample_c1.zip', 'WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', V2.21.01.00899-2P02-14_20210825191325.ospf-128-37667662.lzma', 'ospf@899-2P02-14.tar', '5b89655f43e4da08ed9049ba8cb7f4
DSA         1004 PEM         THUE         FALSE          ["sample_C1.ip", YMMe[rsd]/hersion/YEF/105W042.107.088.170084.556(p/, 105WV2.21.07.088.170084.556(p/, 105WV2.21.07.088.170084.566(p/, 105WV2.21.07.088.170084.57004.566(p/, 105WV2.21.07.088.170084.566(p/, 105WV2.21	DSA	1024 PEM	TRUE	FALSE '			['sample_C1.zip', WVMe/docker/overlay2/0a3d8212dfe3562133348ad9928fef77aaab1fabdae4f05d464111e982d1e342/dfff/etc/ssh/ssh_host_dsa_key']
0 PEM         TRUE         TRUE <t< td=""><td>RSA</td><td>2048 PEM</td><td>TRUE</td><td>FALSE '</td><td></td><td></td><td>['sample_c1.zip', 'WVMe/docker/overlay2/0a908212dfe356213548ad9928fef77aaab1fabdae4105d464111e982d1e3x2/diff/tetc/ssh/ssh_host_rsa_key]</td></t<>	RSA	2048 PEM	TRUE	FALSE '			['sample_c1.zip', 'WVMe/docker/overlay2/0a908212dfe356213548ad9928fef77aaab1fabdae4105d464111e982d1e3x2/diff/tetc/ssh/ssh_host_rsa_key]
0 PEM         TRUE         TRUE         Image         ["sample_CLaip", WMe/ssl/hesion/VE/V/210.00899-3P02-14_202082519125.ospl", V22.01.00899-3P02-14_202082519125.ospl", V22.01.00899-	DSA	1024 PEM	TRUE	FALSE '			['sample_C1.zip', WVMe/ssd/1/version/VER/105WV2.21.07.08817D0824 5g_A56224526Cpu', 105WV2.21.07.08817D0824 5g_A56224526Cpu-4109630-23357403.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/ssh/ssh_host_dsa ke
RSA         2048 PEM         TRUE         FALSE          ["sample_C1.zip", WM/e/docker/overlag/2/8d95568356bdees/855708556f1abc/ff4bad061374eArTBA4Bad9060007/dff1/home/webmrt/config/beegu.X           RSA         2048 PEM         TRUE         FALSE          ["sample_C1.zip", WM/e/docker/overlag/2/8d95568356bdees/855708556f1abc/ff4bad061374eArTBA4Bad9060007/dff1/home/webmrt/config/beegu.X           RSA         2048 PEM         TRUE         FALSE          ["sample_C1.zip", WM/e/docker/overlag/2/8d9556856bdees/855708556f1abc/ff4bad061374eArTBA4Bad9060007/dff1/home/webmrt/config/beegu.X           RSA         2048 PEM         TRUE         FALSE          ["sample_C1.zip", WM/e/sd0/Lip"/sd0/L		0 PEM	TRUE	TRUE '			['sample_c1.zip', 'WVMe/registry/docker/docker/docker/setsion/v2/blobs/sha256/cr/cx844d37e5318f3b783e9e520d22a79fe7840b4d14f9d72d96eeed25a58153cd/data', version/lib/librosng.so]
RSA         2048 PEM         TRUE         FALSE         Image: Claip:         Image: Claip: NVMe/socker/overlag/26d9556856956bdes58573655861abccHf4abd0613748+zHa4be060071dff/home/webmrl; config/server.k           RSA         2048 PEM         TRUE         FALSE         Image: Claip: NVMe/socker/overlag/26d9556856bdes58573655861abccHf4abd0613748+zHa4be060071dff/home/webmrl; config/server.k           RSA         2048 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/estor/NVFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3           RSA         2048 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/estor/NVFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3           RSA         2048 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/version/VEFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3           RSA         1004 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/version/VEFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3           RSA         2049 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/version/VEFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3           RSA         2049 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/version/VEFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3           RSA         2049 PEM         TRUE         FALSE         Image: Claip: NVMe/soc/1/version/VEFX/221.01.00895-3701-14_20120035191325.webmrl: 128-3		0 PEM	TRUE	TRUE '			['sample_C1.zip', 'WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899-2P02-14_20210825191325.ospf-128-37667662.lzma', 'ospf@B99-2P02-14.tar', '5b89c55f43e4da08ed90a9ba8ecb7H
ASA         2048 PEM         TRUE         FALSE          ["sample_C1.zip", WMe/ssd1/hersion/VEX/V2.10.00899-2902-14_2021082519125.webmmt, V2.21.01.00899-2902-14_2021082519125.webmmt, V2.21.01.0089-2902-14_2021082519125.webmmt, V2.21.01.00899-2902-14_2021082519125.webmmt, V2.21.01.00899-2902-14_202108	RSA	2048 PEM	TRUE	FALSE '			['sample_CL.zip', NVMe[docker/overlay2]8d9b5686369bb8ee5a95c7366566fafb0cbff4bab0618748e47fa348a9e06007/diff/home/webmnt/config/beego.key]
AND PERM         TRUE         FALSE          ["sample_C1.zip", WMMe/ssd/L/hersion/VEF/V.21.00.00899-3900-14_2021002519132S.webmmt, V.21.00.00899-3900-14_2021002519132S.webmmt,	RSA	2048 PEM	TRUE	FALSE '			['sample_c1.zip', 'WVMe/docker/overlay2/8d9b5866369bb8e65a95c73685566fafb0cbff4bab0618748e47fa348a9e06007/diff/home/webmnt/config/server.key]
RSA         1024 PEM         TRUE         FALSE          ["sample_C1.zip", WMe/registry/locker/docker/registry/l2blobs/sh256/c/c/s94437e531856/m32e6253022274F78404d149572d98eee02555325c           RSA         1024 PEM         TRUE         FALSE          ["sample_C1.zip", WMe/registry/locker/docker/registry/l2blobs/sh256/s561525c         000099-2002-14_2020080292002-14_20200292002-14_2020080292002-14_2020080292002-14_20200292002-14_2020080292002-14_2020080292002-14_2020080292002-14_2020080292002-14_2020080292002-14_2020080292002-14_2020080292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_2020029200292002-14_20200292002-14_20200292002-14_20200292002-14_20200292002-14_	RSA	2048 PEM	TRUE	FALSE '			['sample_CL.zip', WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.webmnt', V2.21.01.00899-2P02-14_20210825191325.webmnt-128-36158709.htma', Webmnt@B99-2P02-14.tar', '3a94148b39316830e320
ISA         ID04 PEM         TRUE         FALSE          ["sample_C1.zip", WMe/sol1/version/VEN/v2.10.00899-3P02-14_002082519135.opf, "V2.21.01.00899-3P02-14_002082519135.opf, "V2.21.01.00899-3P02-14_002082519135.opf, "V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf, "V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_002082519135.opf,"V2.21.01.00899-3P02-14_0020825191355.opf,"V2.21.01.008999-3P02-14_0020825193556455680004454580045458004458004458004458004458004458004458004459800445980044598004458004458004459800445980044580044598004459800	RSA	2048 PEM	TRUE	FALSE '			['sample_c1.zip', 'WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.webmnt', V2.21.01.00899-2P02-14_20210825191325.webmnt-128-36158709.lzma', 'webmnt@899-2P02-14_tar', '3a94148b9316830e920
RSA         2048         PEM         TRUE         FALSE         Image: Cl.zip; NVMe/registry/locker/docker/registry	RSA	1024 PEM	TRUE	FALSE '			['sample_CL.zip', 'WVMe/registry/docker/registry/v2/blobs/sha256/cc/cc944d37e5318f5b783e9e520d22a79fe784b04d14f9d72d09eeed25a58t53cd/data', 'version/liib/librosng.so"]
KSA         2048 PEM         TRUE         FALSE         ["sample_C1.zip", WMe/registry/locker/docker/	RSA	1024 PEM	TRUE	FALSE '			['sample_c1.zip', 'WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899-2P02-14_20210825191325.ospf-128-37667662.lzma', 'ospf@899-2P02-14.tar', '5b89b55f43e4da08ed50a9ba8cb7f
KSA 2048 PEM TRUE FALSE ' ['sample_Cl.zip', 'WM/e/ssd/1/version/VER/I05WV2.21.07.0881700824.5g,A9622A528Cpu', 'USWV2.21.07.0881700824.5g,A9622A528Cpu', 'USWV2.21.07.088170824.5g,A9622A528Cpu', 'USWV2.21.07.088170824.5g,A9624.5g,A9624.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5g,A964.5	RSA	2048 PEM	TRUE	FALSE '			['sample_CL.zip', 'WVMe/registry/docker/registry/v2/blobs/sha256/f6/f60e5eae0d89x8b30x4de621c887295490e28400ab0cf0342xcx5c04d9620d21/data', 'home/webmnt/config/beego.key']
	RSA	2048 PEM	TRUE	FALSE '			['sample_c1.zip', 'WVMe/registry/docker/docker/docker/segistry/v2/blobs/sha256/f6/f60e5eae0d89x8b30c4de621c887295490e28400a0cf0342ccc5c4d9620d21/data', 'home/webmnt/config/server.key']
RSA 4096 DER TRUE FALSE	RSA	2048 PEM	TRUE	FALSE '			['sample_c1.zip', 'NVMe/ssd/1/version/VER/105WV2.21.07.08B17D0824_5g.496224526Cpu', '105WV2.21.07.08B17D0824_5g.496224526Cpu-4109630-23357403.gz', 'uboot-fw.img',
	RSA	4096 DER	TRUE	FALSE '			['sample_CLzip', WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325. VswdCpu', V2.21.01.00899-2P02-14_20210825191325. VswdCpu-16821-9438040,gz', V2.21.01.00899-2P02-14_20210825191325. VswdCpu-16821-9438040,gz'
ECDSA 256 PEM TRUE FALSE ' ['sample_C1.zip', YWNe/ssd/1/version/VER/10SWV2.21.07.08817D0824 5g.A9622A526Cpu-/106SW02.21.07.08817D0824 5g.A962XA526Cpu-/106SW02.21.07.08817D0824 5g.A962XA526Cpu-/106SW02.21.07.08817D082050000000000000000000000000000000000	ECDSA	256 PEM	TRUE	FALSE '			['sample_C1.zip', WVMe/ssd/1/version/VER/105WV2.21.07.08817D0824 5g_A9622A526Cpu', 105WV2.21.07.08817D0824_5g_A9622A526Cpu-4109630-23357403.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/ssh/ssh_host_ecdsa
	Cl infoleak-asymmetric-private +	symmetric-private +	-private +	+			

## Figure 25: C1 Asymmetric keys (Black Duck)

Algorithm Bi				Content Use			File File
RSA	4096 PEM	FALSE	FALSE			1 TRUE	
RSA	2048 PEM	FALSE	FALSE			1: TRUE	
RSA	2048 PEM	FALSE	FALSE			-0. TRUE	
RSA	2048 PEM	FALSE	FALSE			-3 TRUE	
ISA	4096 PEM	FALSE	FALSE		2038-07		
CDSA	384 PEM	FALSE	FALSE			1: TRUE	
ISA	2048 PEM	FALSE	FALSE		2029-12		
SA	4096 PEM	FALSE	FALSE		2042-02	-0 TRUE	
SA	1024 PEM	FALSE	FALSE				['sample_CL.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/40/40d2da04645426b9
ISA	4095 PEM	FALSE	FALSE			1. TRUE	
ISA	2048 PEM	FALSE	FALSE	·	2025-05	1 TRUE	
ISA	2048 PEM	FALSE	FALSE	·	2037-12	-0: TRUE	
RSA	2048 PEM	FALSE	FALSE	·	2029-12	-3: TRUE	
ISA	4096 PEM	FALSE	FALSE	·	2038-07	-3: TRUE	['countryName': "EU", "localityName': "Madrid (see current address at www.camerfirma.com/address)", "serialNumber': "A&['sample_C1.zip', "NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b'
CDSA	384 PEM	FALSE	FALSE	·	2038-01	1 TRUE	["countryName": "US", "organizationName": "VeriSign, Inc.", "organizationalUnitName": "(c) 2007 VeriSign, Inc For authorize ['sample_c1.zip', "NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b
ISA	2048 PEM	FALSE	FALSE	·	2029-12	-3 TRUE	["countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sy: ['sample_c1.zip', "NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b"
RSA	4096 PEM	FALSE	FALSE	Sec	2042-02	0 TRUE	["countryName": "RO", "organizationName": "CERTSIGN SA", "organizationalUnitName": "certSIGN ROOT CA G2"] ['sample_C1.zip', "NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b"
RSA	4096 PEM	FALSE	FALSE	·	2042-01	1 TRUE	["countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 G3"] [Sample_C1.zip', "NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepaasccm", V2.21
RSA	2048 PEM	FALSE	FALSE	·	2025-05	1 TRUE	["countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimor ['sample_C1.zip', "NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepaasccm', V2.2:
RSA	2048 PEM	FALSE	FALSE	·	2037-12	0: TRUE	["countryName": "US", "organizationName": "VeriSign, Inc.", "organizationalUnitName": "(c) 2008 VeriSign, Inc For authorize ['sample_c1.zip', "NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepaasccm", V2.2:
RSA	2048 PEM	FALSE	FALSE	·	2029-12	-3 TRUE	["countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COM ['sample_c1.zip', "NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepaasccm", V2.21
ISA	4095 PEM	FALSE	FALSE		2038-07	-3 TRUE	["countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "AE["sample_L1_zip', "NVMe/ssd/1/swm/VER/V2_21_01_00899-2P02-14_20210825191325.litepaasccm', V2_21
RSA	2048 PEM	FALSE	FALSE	Sec. 1	2029-12	3 TRUE	["countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sy: ['sample_c1.zip', "NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepaasccm', V2.21
ISA	4096 PEM	FALSE	FALSE	·	2042-02	0 TRUE	["countryName": "RO", "organizationName": "CERTSIGN SA", "organizationalUnitName": "certSIGN ROOT CA G2"} ['sample_C1.zip', 'NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepaasccm', V2.21
RSA	4096 PEM	FALSE	FALSE	L	2042-01	1 TRUE	["countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 G3"} [['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.VswdCpu', 'V2.2'
RSA	2048 PEM	FALSE	FALSE	L	2025-05	1 TRUE	["countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimor ['sample_c1.zip', "NVMe/ssd/1/version/VER/v2.21.01.00899-2P02-14_20210825191325.VswdCpu', V2.22
RSA	2048 PEM	FALSE	FALSE	L	2037-12	0 TRUE	["countryName": "US", "organizationName": "VeriSign, Inc.", "organizationalUnitName": "(c) 2008 VeriSign, Inc For authorize ['sample_C1.zip', "WVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325. VswdCpu', 'V2.2
ISA	2048 PEM	FALSE	FALSE	L	2029-12	-3 TRUE	["countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COM ['sample_CL2ip', "NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210825191325.VswdCpu', 'V2.2
ISA	4096 PEM	FALSE	FALSE	S	2038-07	3 TRUE	["countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address]", "serialNumber": "AE ['sample_CL_zip', "NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210825191325.VswdCpu', 'V2.2
ISA	2048 PEM	FALSE	FALSE	·	2029-12	3 TRUE	["countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sy: [Sample C1.zip', "NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14 20210825191325.VswdCpu', V2.2
RSA	4096 PEM	FALSE	FALSE	·	2042-02	O TRUE	
ISA	4096 PEM	FALSE	FALSE	·	2042-01	1 TRUE	
RSA	2048 PEM	FALSE	FALSE	·	2025-05	1 TRUE	["countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimor [Sample Cl.zip', "NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14 20210825191325.VswdCpu', V2.2
RSA	2048 PEM	FALSE	FAISE		2027.42	O TRUE	

### Figure 26: Symmetric keys (Black Duck)

10639 statvfs@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/sftp']
10640 aes128-gcm@openssh.com	['sample_c1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh']
10641 ssh-dss-cert-v01@openssh.com	['sample_c1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh']
10642 hmac-md5-etm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh']
10643 aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-adc
10644 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-adc
10645 aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-age
10646 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-age
10647 aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-key
10648 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/docker/overlay2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa069465d4/diff/usr/bin/ssh-keygen']
10649 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-key
10650 aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-key
10651 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-key
10652 hmac-md5-etm@openssh.com	['sample C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-key
10653 aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/libexec/opc
10654 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/libexec/opc
10655 hmac-md5-etm@openssh.com	l'sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/libexec/opt
10656 tz@iana.org	['sample_C1.zip', 'NVMe/registry/docker/registry/v2/blobs/sha256/c5/c5bf7f535721157f9896330806d77ad7470dfbf3a2cd8603a9d21071482be19b/data', 'sbin/zdump']
10657 mbj@tail-f.com	I'sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10658 j.schoenwaelder@jacobs-university.de	['sample_C1.zip', 'NVMe/registry/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10659 aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/docker/overlav2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa069465d4/diff/usr/bin/ssh-kevscan']
10660 mbj@tail-f.com	'sample_C1.tip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10661 mbj@tail-f.com	'sample_C1.zip', 'NVMe/registrv/docker/docker/registrv/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10662 ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/docker/overlav2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa009465d4/diff/usr/bin/ssh-kevscan']
10663 hmac-md5-etm@openssh.com	['sample_C1.zip', 'NVMe/docker/overlav2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa069465d4/diff/usr/bin/ssh-kevscan']
10664 j.schoenwaelder@jacobs-university.de	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10665 mbj@tail-f.com	Isample_C1.zip', NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26ddfad5f893da1345402a557b406a/data', 'ROSNG/script.
10666 j.schoenwaelder@jacobs-university.de	['sample C1.zip', NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', ROSNG/script.
10667 J.schoenwaelder@jacobs-university.de	Isample_C1.zip', NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script_
10668 j.schoenwaelder@jacobs-university.de	[sample Cl.zip', NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd20d4fad5f893da1345402a557b406a/data', ROSNG/script
10669 10026717@zte.com.cn	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d5/d5126299abcf6f4f4cbaeca01800955e2bc68a60f87d3ad77eac81ffbbaaf4a8/data']
10670 tz@iana.org	[ sample Cl.zb/, NVMe/registry/docker/docker/registry/v2/blobs/sha256/d5/d549b86ea8ce62b9e69d41d28a94e2bc88a8514406e117318a497fce36a83/data', 'sbin/zdump']
10671 10026717@zte.com.cn	[sample_Clap], WWe/registry/docker/docker/docker/segistry/v2/blobs/sha256/d5/d58b8efc97c5dbb2008855c73545a1c4946bce6ee255d723a88ae47a8c0e8d/data']
10672 statyfs@openssh.com	[ sample_Claip, NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc848708375179b616506250473806caecc4/data,'usr/bin/sftp']
10673 aes128-gcm@openssh.com	Lample_C.Lip, 'WWergeistry/docker/docker/egistry/v2/biobs/sha256/d7/d77ac110eb74fb7ffc848708375179b616506a75b81229d7f349780ceacc14/data', 'usr/bin/ssh'
10674 ssh-dss-cert-v01@openssh.com	[sample Cl.:p], 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc848708375179b616506a7f3b81e29d7f349780ceact4/data', 'usr/bin/ssh]
10675 hmac-md5-etm@openssh.com	[ sample_Cl.zb, WWe/registry/docker/docker/registry/v2/biobs/sha256/d7/d7ac110eb74h5/fts34870837579b616506a75b81e29d7549780ceacc14/data', usr/bin/ssh']
10676 aes128-gcm@openssh.com	[sample_C.i.p), NVMe/registry/occeer/occer/registry/v2/blobs/sha256/d7/d7rac110eb74fb7ffcs48708373179b616506a7f3b81c29d7f49780cceac14/data', 'usr/bin/ssh-add
10677 ssh-dss-cert-v01@openssh.com	[ sample_Cl.zip, 'WWe/registry/docker/docker/registry/v2/biobs/sha256/d7/d7ac110eb74/b7ffcs34870857579b616506a75b81e29d7f349780ceacc14/data, 'usr/bin/ssh-add
10678 aes128-gcm@openssh.com	[sample_C.r.n), hwweregistry/occeer/occer/egistry/v2/blobs/sha256/d7/d7rac110eb74fb7ffcs48708375179b61506a74581te29d7f49780ceacc14/data', usr/bin/ssh-age
10679 ssh-dss-cert-v01@openssh.com	[ sample_Cl.zip, 'NVMe/registry/docker/docker/registry/v2/biobs/sha256/d7/d7ac110eb74/hD7ffc848708575179b616506a75081292d7f48780ceacc14/data', 'usr/bin/ssh-age
10680 aes128-gcm@openssh.com	[sample_Lizp], Www/registry/docker/docker/registry/2/blobs/sha256/d7/d77ac110eb74h57ftc83a8708375179b61506a7f3b81e29d749780ceacLa/data, usr/bin/ssh-key [sample_Lizp], WVM/registry/docker/docker/registry/2/blobs/sha256/d7/d77ac110eb74h57ftc83a8708375179b61506a7f3b81e29d7f349780ceacLa/data, usr/bin/ssh-key
10681 ssh-dss-cert-v01@openssh.com	[ sample_C1.zb/, NVMe/registry/docker/docker/docker/docker/sgistry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc8348708375179b616506a7f3b81e29d7f34780ceacc14/data', 'usr/bin/ssh-key
10682 aes128-gcm@openssh.com	[ sample_1.izp], 'WW#/registry/docker/docker/registry/2/blobs/sha256/d7/d77ac110eb74fb7ffc8348708375179b616506a73b81e29d7349780cceecta/udut, usr/bin/ssh-key ['sample_1.izp', 'WV#/registry/docker/docker/registry/2/blobs/sha256/d7/d77ac110eb74fb7ffc8348708375179b616506a73b81e29d7349780cceecta/data', 'usr/bin/ssh-key
10683 ssh-dss-cert-v01@openssh.com	[ sample_L1.zip , 'www/registry/docker/active/registry/v2/biobs/sha256/d7/d77ac110e/afb7fc8348708375179b616506a73b81e29d749780ceactiv/data, usr/bin/ssh-key ['sample_L1.zip', 'WVM/registry/docker/docker/registry/v2/biobs/sha256/d7/d77ac110e/afb7ffc8348708375179b616506a73b81e29d749780ceactiv/data, 'usr/bin/ssh-key
10683 ssn-dss-cert-v01@openssh.com 10684 hmac-md5-etm@openssh.com	[sample_L.1.ip; NVMer/registry/docker/registry/v2/biobs/sha256/d7/d77ac110e5/4h5/rt6348/083/51/9b61506d73b1e29d7349/80ceacc14/data; 'usr/bin/ssh-key [Sample_L1.ip; 'NVMer/registry/docker/registry/v2/biobs/sha256/d7/d77ac110e5/4h5/rt6348/083751/9b61506d73b1e29d73497B0ceacc14/data; 'usr/bin/ssh-key
	[sample_L.zip; NVMerregistty/docker/registty/v2/biobs/sha256/d7/d77ac110eb/ah2/ft6348/08375179bb15006/af3bite29d749780ceacc14/data; 'usr/binyssh-keyp [sample_L.zip; 'NVMerregistty/docker/registty/v2/biobs/sha256/d7/d77ac110eb/ah2/ft6348/08375179bb1506af3bite29d749780ceacc14/data; 'usr/binyssh-keyp
10685 aes128-gcm@openssh.com 10686 ssh-dss-cert-v01@openssh.com	[sample_Cl.th], NVMe/registry/docker/docker/registry/v2/biobs/sha256/d7/d7act10e/a/bio/a/s0/06/51/5001500a/35050220/7395700000000000000000000000000000000000

Figure 27: C1 Infoleak email addresses (Black Duck)

A	В	С	D	E	F	G	Н	1	J	K	L	M	N	0
IP	IPv6	File												
192.254.1.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/006973	3cb60337259	0bd4308	5960e012b3	bd54b61d	bf8906eab	f9a487126	5997d/con	fig.v2.jso
192.254.128.1	FALSE			NVMe/docke										
173.254.128.2	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/006973	3cb60337259	0bd4308	5960e012b3	bd54b61d	bf8906eab	f9a487126	5997d/con	fig.v2.jso
173.254.95.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/006973	3cb60337259	0bd4308	5960e012b3	bd54b61d	bf8906eab	f9a487126	5997d/con	fig.v2.jso
192.254.1.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/00cf7a	27cb921146	ff9fcc91f2	259122adb6	6287d1c6d	lab2635ecf	1881a8a09	9d/config	.v2.json']
192.254.128.1	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/00cf7a	27cb921146	ff9fcc91f2	259122adb6	6287d1c6d	lab2635ecf	1881a8a09	9d/config	.v2.json']
173.254.128.2	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/00cf7a	27cb921146	ff9fcc91f2	259122adb6	6287d1c6d	lab2635ecf	1881a8a09	9d/config	.v2.json']
173.254.95.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/00cf7a	27cb921146	ff9fcc91f2	259122adb6	6287d1c6d	lab2635ecf	1881a8a09	9d/config	.v2.json']
192.254.1.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/02dc6f	3b9ca93537	1226cbe7	ccd8286a01	2544c6e09	9634066d00	bf2f9f1c1	b47/config	g.v2.json']
192.254.128.1	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/02dc6f	3b9ca93537	1226cbe7	ccd8286a01	2544c6e09	9634066d00	bf2f9f1c1	b47/config	g.v2.json'
173.254.128.2	FALSE	['sample	C1.zip', '	NVMe/docke	er/containe	ers/02dc6f	3b9ca93537	1226cbe7	ccd8286a01	2544c6e09	9634066d00	bf2f9f1c1	b47/config	.v2.json']
173.254.95.16	FALSE	['sample	C1.zip', '	NVMe/docke	er/containe	ers/02dc6f	3b9ca93537	1226cbe7	ccd8286a01	2544c6e09	9634066d00	bf2f9f1c1	b47/config	z.v2.json'
192.254.1.16	FALSE	['sample	C1.zip', '	NVMe/docke	er/containe	ers/04f025	8734e2c96e	e67dfc8c	0f2e6901d5	f427dc0cd	db6433025	0be54455f	005/confi	g.v2.json'
192.254.128.1	FALSE	· · -		NVMe/docke										
173.254.128.2	FALSE			NVMe/docke										· ·
173.254.95.16	FALSE			, NVMe/docke										· ·
192.254.1.16	FALSE			NVMe/docke		-								<b>·</b> ·
173.254.95.16	FALSE			NVMe/docke										
127.0.0.1	FALSE			NVMe/docke										
8.8.8.8	FALSE			NVMe/docke										
3.8.4.4	FALSE			NVMe/docke										
192.254.1.16	FALSE	· · -		NVMe/docke										
173.254.95.16	FALSE			NVMe/docke										· ·
127.0.0.1	FALSE			NVMe/docke										· ·
8.8.8.8	FALSE			NVMe/docke										
3.8.4.4	FALSE	· · -		NVMe/docke										
8.8.4.4 192.254.1.16	FALSE			NVMe/docke										
192.254.128.1	FALSE			NVMe/docke										
173.254.128.2	FALSE	· · -		NVMe/docke										
173.254.95.16	FALSE			NVMe/docke										
192.254.1.16	FALSE			NVMe/docke										
173.254.95.16	FALSE			NVMe/docke		-								
127.0.0.1	FALSE	· · -		NVMe/docke										•
8.8.8.8	FALSE			NVMe/docke										
8.8.4.4	FALSE			NVMe/docke										
192.254.1.16	FALSE			NVMe/docke										· ·
192.254.128.1	FALSE	· · -		NVMe/docke										· ·
173.254.128.2	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/0f55a6	bc61a68c66	7a96230c	f80bc42fd5	d9589427a	5b86b205e	3ef8033a5	570/confi	g.v2.json
173.254.95.16	FALSE			NVMe/docke										
192.254.1.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/101cfa	c99cd65d36	0e867aa3	66c6433c49	a980e81a2	28af32ed89	5a8f3a3b8	c73/config	g.v2.json
192.254.128.1	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/101cfa	c99cd65d36	0e867aa3	66c6433c49	a980e81a2	28af32ed89	5a8f3a3b8	c73/config	g.v2.json'
173.254.128.2	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/101cfa	c99cd65d36	0e867aa3	66c6433c49	a980e81a2	28af32ed89	5a8f3a3b8	c73/config	g.v2.json
173.254.95.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/101cfa	c99cd65d36	0e867aa3	66c6433c49	a980e81a2	28af32ed89	5a8f3a3b8	c73/config	g.v2.json'
192.254.1.16	FALSE	['sample_	C1.zip', '	NVMe/docke	er/containe	ers/10e409	91610c5422a	6f9f0407	076e12202d	lec28e45fa	a2a9390269	bbe2a4f17	7715/confi	g.v2.json
192.254.128.1	FALSE	['sample	C1.zip', '	NVMe/docke	er/containe	ers/10e409	91610c5422a	6f9f0407	076e12202d	lec28e45fa	a2a9390269	bbe2a4f17	7715/confi	g.v2.json
173.254.128.2	FALSE	['sample	C1.zip', '	NVMe/docke	er/containe	ers/10e40	91610c5422a	of9f0407	076e12202d	lec28e45fa	a2a9390269	bbe2a4f17	7715/confi	g.v2.json

Figure 28: C1 Infoleak IP addresses (Black Duck)

Vendor MICRO-STAR INT'L CO.,LTD. Officially Xerox CIMSYS Inc		ip', 'NVMe/ssd/	1/worrign/														
Officially Xerox		ip', 'NVMe/ssd/															
CIMSYS Inc		ip', 'NVMe/ssd/													', 'ospt@B99-	2P02-14.tar	', '9b785
		ip', 'NVMe/dock															
ZHONGXING TELECOM LTD.		ip', 'NVMe/dock															
CIMSYS Inc		ip', 'NVMe/dock															
CIMSYS Inc		ip', 'NVMe/dock															
CIMSYS Inc																	
CIMSYS Inc																	
CIMSYS Inc	['sample_C1.a	ip', 'NVMe/dock	<pre>(er/overlay)</pre>	/2/dbb0948	0363834b912	d9f8f0cd0e	e9efe67b	1d76ae2	leacb2b8	b5f673f154e	9c/diff/et	c/network/	interfaces'	]			
ZHONGXING TELECOM LTD.	['sample_C1.a	ip', 'NVMe/logs/	/BSP/Board	dInit.log.ba	k.1', 'BoardIr	nit.log.bak']											
ZHONGXING TELECOM LTD.	['sample_C1.a	ip', 'NVMe/logs/	/BSP/Board	dInit.log.ba	k.2', 'BoardIr	it.log.bak']											
Intel	['sample_C1.a	ip', 'NVMe/logs/	/BSP/BspM	Ioni.log']													
ASIX ELECTRONICS CORP.	['sample_C1.a	ip', 'NVMe/logs/	/BSP/BspM	Ioni.log']													
ASIX ELECTRONICS CORP.	['sample_C1.a	ip', 'NVMe/logs/	/BSP/BspM	loni.log']													
ASIX ELECTRONICS CORP.	['sample C1.a	ip', 'NVMe/logs/	/BSP/BspM	loni.log']													
Micro-Star INTL CO., LTD.	['sample_C1.a	ip', 'NVMe/logs	/BSP/BspM	Ioni.log'l													
ASIX ELECTRONICS CORP.																	
ASIX ELECTRONICS CORP.																	
ASIX ELECTRONICS CORP.																	
ASIX ELECTRONICS CORP.	['sample_C1.a	ip', 'NVMe/logs/	/BSP/BspM	loni.log']													
ASIX ELECTRONICS CORP.																	
Liteon																	
Officially Xerox	['sample_C1.a	ip', 'NVMe/logs/	/BSP/BspM	Ioni.log']													
Intel	['sample_C1.a	ip', 'NVMe/logs/	/BSP/BspM	loni.log']													
Officially Xerox	['sample_C1.a	ip', 'NVMe/logs/	/BSP/VbpB	roken8.log	1												
Officially Xerox	['sample_C1.a	ip', 'NVMe/logs/	/litepaas/l	pmslave.lo	g']												
CIMSYS Inc	['sample C1.a	ip', 'NVMe/regis	stry/docker	r/docker/re	gistry/v2/bl	obs/sha256	/of/of345	c9514ad0	04316ae23	a03476fb40	352b338b8	332a736bbd	be48c8552	a8fb6/data	'etc.nommu	/network/ir	nterfac
	CINKYS INC CINKYS INC CINKYS INC CINKYS INC CHONGXING TELECOM LTD. CHONGXING TELECOM LTD. CHONGXING TELECOM LTD. CHONGXING TELECOM LTD. CINKYS CINKYS CORP. CINKYS CONSTANTS	CIMSYS Inc     ['sample_Cl.:       CIMSYS Inc     ['sample_Cl.:       CIMSYS Inc     ['sample_Cl.:       CHONGXING TELECOM LTD.     ['sample_Cl.:       ZHONGXING TELECOM LTD.     ['sample_Cl.:       CHONGXING TELECOM LTD.     ['sample_Cl.:       SIX ELECTRONICS CORP.     ['sample_Cl.:   <	CIMSYS Inc         ['sample_CL12P', NVMe/dot           CIMSYS Inc         ['sample_CL12P', NVMe/dot           CIMSYS Inc         ['sample_CL12P', NVMe/dot           CIMSYS Inc         ['sample_CL12P', NVMe/logs           CIMSYS Inc         ['sample_CL12P', NVMe/logs           SIM CETERONICS CORP.         ['sample_CL12P', NVMe/logs           SIM ELETERONICS CORP.         ['s	CIMSTS Inc         ['sample_C.1.2ip', 'NVMe/docker/overlap, CLMSTS Inc         ['sample_C.1.2ip', 'NVMe/docker/overlap, CLMSTS Inc           CLMSTS Inc         ['sample_C.1.2ip', 'NVMe/docker/overlap, CLMSTS Inc         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, Intel           CLMSTS Inc         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, Intel         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, SBS ELECTRONICS CORP,           SISK ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, SBS ELECTRONICS CORP,           SISK ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Baor, SBS ELECTRONICS CORP,           SISK ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,           SISK ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,           DUP INTERNATIONAL         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,           SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,           SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS CORP,         ['sample_C.1.2ip', 'NVMe/logs/SBS/Babr, SBS ELECTRONICS	CIMSYS Inc         ['sample_Cl.zip', NVMe/docker/overlay/D697A38           CIMSYS Inc         ['sample_Cl.zip', NVMe/docker/overlay/D697A38           CIMSYS Inc         ['sample_Cl.zip', NVMe/logs/BSP/Boardint.log.ba           CHONGXING TELECOM LTD.         ['sample_Cl.zip', NVMe/logs/BSP/Boardint.log.ba           CHONGXING TELECOM LTD.         ['sample_Cl.zip', NVMe/logs/BSP/Boardint.log.ba           DRIONGXING TELECOM LTD.         ['sample_Cl.zip', NVMe/logs/BSP/Boardint.log.ba           SIX ELETCONICS CORP.         ['sample_Cl.zip', NVMe/logs/BSP/BoANG.log']           SIX ELETCONICS CORP.         ['sample_Cl.zip', NVMe/logs/BSP/BoANG.log']           SIX ELETCONICS CORP.         ['sample_Cl.zip', NVMe/logs/BSP/BoANG.log']           SIX ELETCONICS CORP.         ['sample_Cl.zip', NVMe/logs/BSP/BSP/BoANG.log']           SIX ELETCONICS CORP.         ['sample_Cl.zip', NVMe/logs/BSP/BSP/BoANG.log']	CIMSYS Inc         ['sample_C.1:p', 'NVMe/docker/overlay2/Get7as30367c064           CIMSYS Inc         ['sample_C.1:p', 'NVMe/docker/overlay2/Get7as30367c064           CIMSYS Inc         ['sample_C.1:p', 'NVMe/docker/overlay2/Get7as30367c064           CIMSYS Inc         ['sample_C.1:p', 'NVMe/logs/SB7/Boardint.1:g, bac.2', 'Boardintel Clay, 'NVMe/logs/SB7/Boardint.1:g, bac.2', 'Boardintel Clay, 'NVMe/logs/SB7/Boardint.1:g, bac.2', 'Boardintel ['sample_C.1:p', 'NVMe/logs/SB7/Boardint.1:g, bac.2', 'Boardintel ['sample_C.1:p', 'NVMe/logs/SB7/Boardint.1:g, bac.2', 'Boardintel SBK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Boanl.1:g']           SBK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/BspMon.1:g']         SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/BspMon.1:g']           SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs9/BspMon.1:g']         SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs9/Bs0.1:g']           SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs9/Bs0.1:g']         SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs9/Bs0.1:g']           SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0.1:g']         SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0.1:g']           SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0.1:g']         SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0.1:g']           Liteon         ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0.1:g']         SSK ELECTRONICS CORP. ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0.1:g']           Liteon         ['sample_C.1:p', 'NVMe/logs/SB7/Bs9/Bs0	CIMSYS Inc         Tsample         Clarp:         NVMe/focker/overlay/Ded7a333367c0d5dea1146d           CIMSYS Inc         ['sample_Clarp', NVMe/fock/set/overlay/Ded7a33367c0d5dea1146d           CIMSYS Inc         ['sample_Clarp', NVMe/fock/set/overlay/Ded7a33367c0d5dea1146d           CIMSYS Inc         ['sample_Clarp', NVMe/fock/set/Set/Boardint.log.bat.1, 'Boardint.log.bat.1, 'Boardint.log.bat.1, 'Boardint.log.bat.2, 'Boardint.log.'Boardint.log.bat.2, 'Boardint.log.bat.2, 'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.'Boardint.log.bat.2, 'Boardint.log.'Boardint.lo	CIMSYS Inc         ['sample_C.L.ip', 'NVMe/locker/overlay2/ed73833857c0655dae114648eea301.           CIMSYS Inc         ['sample_C.L.ip', 'NVMe/log/SP/SordiniLog.bak.1', 'BoardiniLog.bak.1', 'Bo	CIMSYS Inc         ['sample_Clip', 'NVMe/docker/overlay/Ded/3839867cd05d6e1146d48ee30311427c67           CIMSYS Inc         ['sample_Clip', 'NVMe/docker/overlay/Ded/3839867cd05d6e1146d48ee30311427c67           CIMSYS Inc         ['sample_Clip', 'NVMe/docker/overlay/Ded/3839867cd05d6e31146d28ee303147c67           CHONSXING TELECOM LTD.         ['sample_Clip', 'NVMe/dock/SS/Boardint.Log.bak1,' Boardint.Log.bak1           CHONSXING TELECOM LTD.         ['sample_Clip', 'NVMe/dock/SS/SB/Boardint.Log.bak2,' Boardint.Log.bak1           Tell         ['sample_Clip', 'NVMe/dock/SS/SB/Boardint.Log.bak2,' Boardint.Log.bak2,' Boardint.Log.bak2,	CIMSYS Inc         ["sample_C.l.zip", NVMe/logker/overlay2/deb38393b37cdb5d4aee1146d48ee0301472cf7438b0cb           CIMSYS Inc         ["sample_C.l.zip", NVMe/logk/BSP/boardInit.log.bak.1", BoardInit.log.bak.1]           CIMSYS Inc         ["sample_C.l.zip", NVMe/logk/BSP/boardInit.log.bak.1", BoardInit.log.bak.1]           CIMSYS Inc         ["sample_C.l.zip", NVMe/logk/BSP/boardInit.log.bak.2", BoardInit.log.bak.2]           CIMSYS Inc         ["sample_C.l.zip", NVMe/logk/BSP/boardInit.log.bak.2", BoardInit.log.bak.2]           CIMSYS Inc         ["sample_C.l.zip", NVMe/logk/BSP/BSPMon.log"]           SIX ELECTRONICS CORP.         ["sample_C.l.zip", NVMe/logk/BSP/BSPMon.log"]	CIMSYS Inc         ["sample_C.1:ip", NVMe/logker/overlay2/6erJ38393b7cdb5d48ee031475cdc5de8ee031475cdc5de8e051475cdc5de8e051475cdc6de8e15cd5de8e051475cdc6de8e15cd7d5de8e051475cdc6de8e15cd7d5de8e15cd5de8e15cd7d5de8e15cd5de8e15cd7d5de8e15cd5de8e15cd7d5de8e15cd5de8e15cd7d5de8e15cd5de8e15cd7d5de8e15cd5de8e15cd7d5d8d5d85d5d8d5d8d5d8d5d8d5d8d5d8d5d8d	CIMSYS Inc         ['sample_[C.1.ip', 'NVMe/[docker/overlay2/b604693393b37c0d5dae1.1d6d48eae3031142765421eacb28b5f673154e9c/diff/etC           CIMSYS Inc         ['sample_[C.1.ip', 'NVMe/[docker/overlay2/b60469363843b12d9f8f0c0deesefe67b1d76e21eacb28b5f673154e9c/diff/etC           CIMSYS Inc         ['sample_[C.1.ip', 'NVMe/[docker/overlay2/b60469363843b12d9f8f0c0deesefe67b1d76e21eacb28b5f673154e9c/diff/etC           CIMSYS Inc         ['sample_[C.1.ip', 'NVMe/[docker/overlay2/b60469163e34b12d9f8f0c0deesefe67b1d76e21eacb28b5f673154e9c/diff/etC           CIMSYS INC         ['sample_[C.1.ip', 'NVMe/[docker/overlay2/b604601.lg']           CIMSYS INC         ['sample_[C.1.ip', 'NVMe/[docker/overlay2/b678b9f86001.lg']           SKE ELETCRONCS CORP.         ['sample_[C.1.ip', 'NVMe/[dock/859/858/Mon1.lg']           SKE ELETCRONCS CORP.         ['sample_[C.1.ip', 'NVMe/[dock/859/858/Mon1.lg']           SKE ELETCRONCS CORP.         ['sample_[C.1.ip', 'NVMe/[dock/859/858/Mon1.lg']           DUP INTERNATIONAL         ['sample_[C.1.ip', 'NVMe/[dock/859/858/Mon1.lg']           SKE ELETCRONCS CORP.         ['sample_[C.1.ip', 'NVMe/[dock/859/858/Mon1.lg']           DUP INTERNATIONAL         ['sample_[C.1.ip', 'NVMe/[dock/859/858/Mon1.lg']	CIMSYS Inc         ['sample_C.Lip', 'NVMe/docker/overlay/2/feb/38393b87cdb5d6ae.031142/c57480bcd9789fbC5fdaaLa/dfffetc/network/           CIMSYS Inc         ['sample_C.Lip', 'NVMe/docker/overlay/2/b6b948036384912d9f8fbcd0ee9e67b1d75ae21excb28b5f673154esc/dff/etc/network/           CHONGXING TELECOM LTD.         ['sample_C.Lip', 'NVMe/logs/B8/PBardninLig_bak1', 'BoardininLig_bak1']           CHONGXING TELECOM LTD.         ['sample_C.Lip', 'NVMe/logs/B8/PBardninLig_bak2', 'BoardininLig_bak1']           CHONGXING TELECOM LTD.         ['sample_C.Lip', 'NVMe/logs/B8/PBardninLig']           SKE ELETGNONCS CORP.         ['sample_C.Lip', 'NVMe/logs/B8/PBardninLig']           SKE ELETONCS CORP.         ['sample_C.Lip', 'NVMe/logs/B8/PBardninLig']           SKE ELETONCS CORP.         ['sample_C.Lip', 'NVMe/logs/B8/P	CIMSYS Inc         Tsample_Cl.1p;         YWMe/docker/overlay2/Get7a8331b87cd5ddae146d48ea901142;0257448bc697969f0c3fdaa1a/diff/etc/network/interfaces'           CIMSYS Inc         ['sample_Cl.1p;         YWMe/docker/overlay2/Get7a8331b87cd5ddae146deae9011472;0248b258b5f673154e9c/diff/etc/network/interfaces'           EMOKXING TELECOM LID.         ['sample_Cl.1p;         YWMe/logs/BSF/BoardiniLlog.bak.';         BoardiniLlog.bak.']           ZHONGXING TELECOM LID.         ['sample_Cl.1p;         YWMe/logs/BSF/BoardiniLlog.bak.']         Common Ling.           ZHONGXING TELECOM LID. </td <td>CIMSYS Inc         [1ample_Cl.1p]; YWMe/docker/overlay2/dochas333b8rcdb5dae146448ee3011427c56-7480bc097990c3fdaa1a/diff/etc/network/interfaces7           CLMSYS Inc         [1ample_Cl.1p]; YWMe/docker/overlay2/dbc09480363834b9ardintLlog.bak1;         [1ample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;           CLMSXIN TELECON LD.         ['tample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;         [Iample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;           PRIONXINT TELECON LD.         ['tample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;         [Iample_Cl.1p]; YWMe/logs/BSP/BoyMonLlog]           SKE ELETCRONCS CORP.         ['tample_Cl.1p]; YWMe/logs/BSP/BoyMonLlog]         [Iample_Cl.1p]; YWMe/logs/BSP/BoyMonLlog]           SKE ELETCRONCS CORP.</td> <td>DIMSY Inc         Sample C.Lip, WWe/docker/overlay/Eed7as33b87cdbddae11ads48ee03114222548bcd799f0c5fdaa1ad/dtf/et/network/interfacer]           DIMSY Inc         Sample C.Lip, WWe/log/SSP/Boardint1.log.bak1         DimSY Inc           DIMONG TELECON ITD.         I'sample C.Lip, WWe/log/SSP/Boardint1.log.bak1         DimSY Inc           DIMONG TELECON ITD.         I'sample C.Lip, WWe/log/SSP/Boardint1.log.bak1         DimSY Inc           DIMONG TELECON ITD.         I'sample C.Lip, WWe/log/SSP/Bpandint.log         DimSY Inc           SIR ELETCRONCS CORP.         Sample C.Lip, WWe/log/SSP/Bpandint.log         DimSY Inc           SIR ELETCRONCS</td> <td>Dissopie         Lampie         Lampie         Clampie         <thclampie< th=""> <thclampie< th=""> <thcl< td=""></thcl<></thclampie<></thclampie<></td>	CIMSYS Inc         [1ample_Cl.1p]; YWMe/docker/overlay2/dochas333b8rcdb5dae146448ee3011427c56-7480bc097990c3fdaa1a/diff/etc/network/interfaces7           CLMSYS Inc         [1ample_Cl.1p]; YWMe/docker/overlay2/dbc09480363834b9ardintLlog.bak1;         [1ample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;           CLMSXIN TELECON LD.         ['tample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;         [Iample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;           PRIONXINT TELECON LD.         ['tample_Cl.1p]; YWMe/logs/BSP/BoardintLlog.bak1;         [Iample_Cl.1p]; YWMe/logs/BSP/BoyMonLlog]           SKE ELETCRONCS CORP.         ['tample_Cl.1p]; YWMe/logs/BSP/BoyMonLlog]         [Iample_Cl.1p]; YWMe/logs/BSP/BoyMonLlog]           SKE ELETCRONCS CORP.	DIMSY Inc         Sample C.Lip, WWe/docker/overlay/Eed7as33b87cdbddae11ads48ee03114222548bcd799f0c5fdaa1ad/dtf/et/network/interfacer]           DIMSY Inc         Sample C.Lip, WWe/log/SSP/Boardint1.log.bak1         DimSY Inc           DIMONG TELECON ITD.         I'sample C.Lip, WWe/log/SSP/Boardint1.log.bak1         DimSY Inc           DIMONG TELECON ITD.         I'sample C.Lip, WWe/log/SSP/Boardint1.log.bak1         DimSY Inc           DIMONG TELECON ITD.         I'sample C.Lip, WWe/log/SSP/Bpandint.log         DimSY Inc           SIR ELETCRONCS CORP.         Sample C.Lip, WWe/log/SSP/Bpandint.log         DimSY Inc           SIR ELETCRONCS	Dissopie         Lampie         Lampie         Clampie         Clampie <thclampie< th=""> <thclampie< th=""> <thcl< td=""></thcl<></thclampie<></thclampie<>

### Figure 29: C1 Infoleak MAC addresses (Black Duck)

	A	D	U	υ	C	F
	Password	User	Algorithm	Salted	Hashed	File
1	ff3sXRd5zvleKT1BGkKdMTrc/LI.9EQ8.cuxSYaGx8hZ7TyQpadClR.z/1QsyepviKd6WfQwkcM2nNm8b6xa.	ssh	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g
3	)7mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	zte	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', '
4	)7mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	zte	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210
5	ltcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPocloG/K1nkyQzmGVcf54TGVIZiUrIA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/9c7ba484e32250c008b710c0380cd
5	ltcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPocloG/K1nkyQzmGVcf54TGVIZiUrIA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
	ltcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPocloG/K1nkyQzmGVcf54TGVIZiUrIA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
	ltcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPocloG/K1nkyQzmGVcf54TGVIZiUrlA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210
)	IbBBZofif9uujiALSfniljsuuQu5Pf46ErUovH4Qvi2	sftp	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/0f1f14a89f222d6768aa0ef3b787b
0	IbBBZofif9uujiALSfniljsuuQu5Pf46ErUovH4Qvi2	sftp	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
1	IbBBZofif9uujiALSfniljsuuQu5Pf46ErUovH4Qvi2	sftp	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210
2	sJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', '
3	sJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210
4	8tVEoIOxiI0FBrtOjf3HbJp1QA08twJMj9bnqIxI4nlQU1gvb5WpmMI6epwMWPod3t6p98zvb51w6R/GWv.v/	root	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca74830
5	8tVEoIOxiI0FBrtOjf3HbJp1QA08twJMj9bnqIxI4nlQU1gvb5WpmMI6epwMWPod3t6p98zvb51w6R/GWv.v/	root	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
6	JoTYQbZ5zH3zBsIQ/vGD1Gsk.IFrZlZGI.wnp9EXYf2aYuyMtAE7YwGbfIO78ImfuNYWpCZCEONjpqHIY.rKG0	zte	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g
7	/Y17tW3kiRlADnks0lgyJ0	root	MD5	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210
в	(2UUvX9AN4Cw3yynYUrfc/ZTs0MdteeHAUcXrNvbMwoXobROQxrB2DY2egzesHKQoDHkUxc2FZ90BQ210knTb0	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/b2932820e1aadc06d33a02bf7576
9		zte		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/11b3c3c142b517f63038984224ed
)		root		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/11b3c3c142b517f63038984224ed
1		zte		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/13e9cdf94b15bc8733b86f15e520
2		root		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/13e9cdf94b15bc8733b86f15e520

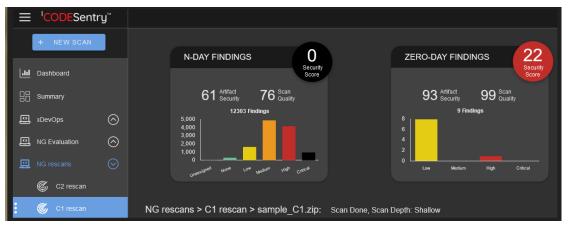
Figure 30: C1 Infoleak passwords (Black Duck)

http://192.254.1.16:8098/api/v1/namespaces/1/rcs/tcfs-log/pods/0	['sample_C1.zip', 'NVMe/docker/containers/ee5a148897f4d755dd2be7105e02dd292abf8472ebec4225c27008bb0afc0d42/con
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/pci/pods/0	['sample_C1.zip', 'NVMe/docker/containers/f57fddac9a94fb7d1ca3cf141edf6b331866ec91eaf97633a3b4793a55372954/config
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/rum/pods/0	['sample_C1.zip', 'NVMe/docker/containers/f630fa98dc8eac61e274426d48127508b77845470620fd5ad01ae5eb2a7a7412/conf
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/usm/pods/0	['sample_C1.zip', 'NVMe/docker/containers/f89b5c4ecc52541e502486174afa795f60a37fe8bffa1265d33f31a2b335913d/config
https://golang.org/wiki/LinuxKernelSignalVectorBug	['sample_C1.zip', 'NVMe/docker/overlay2/0181175375bb1d9b2b617c8f8227c41b568968bba6ed04b873c5bd5176bb6aac/diff/i
https://developers.google.com/protocol-buffers/docs/reference/go/faq#namespace-conflict	['sample_C1.zip', 'NVMe/docker/overlay2/0181175375bb1d9b2b617c8f8227c41b568968bba6ed04b873c5bd5176bb6aac/diff/i
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/026506d26d010b7743fd78ec511adcf01239cc3f9ccef221c58a0b66c2bb5f09/diff/xns
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/026506d26d010b7743fd78ec511adcf01239cc3f9ccef221c58a0b66c2bb5f09/diff/xns
http://www.w3.org/XML/1998/namespaceincorrect	['sample_C1.zip', 'NVMe/docker/overlay2/0290c004c2d150a4551c54c10c027c15c086b1605bdd48f6aee4c8e2bf7fde63/diff/lcs
https://golang.org/wiki/LinuxKernelSignalVectorBug	['sample_C1.zip', 'NVMe/docker/overlay2/03c31222280ccb397f8e326fbf05ebb854b9eab8ffc233340a1c1260db7da9bc/diff/go
http://www.w3.org/XML/1998/namespacejson	['sample_C1.zip', 'NVMe/docker/overlay2/03c31222280ccb397f8e326fbf05ebb854b9eab8ffc233340a1c1260db7da9bc/diff/go
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/390728b66ab39ab9bd999946157d7dc9ca5e39e0ddf7a647b0fe17a58637a484/diff/u
http://redis.io	['sample_C1.zip', 'NVMe/docker/overlay2/39255edd8b9d4e250f604718b3eb2b07c52fbf5c9522544834e92249f3bf457f/diff/re
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/041206d2f319828ed73bee4b37f67d2a186d9f12ec4259320244b2ff64c4ff9c/diff/tcf
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/04c6f6e5929f8f94299fd1ef885208505731648a34e9aab3d8069722ddd3c736/diff/tcf
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/0945c6870d01f657d32a39a4312781f898b92d669cc73e64608d2b4e11ec0b97/diff/ar
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/881cd097b8285eab427f138a7a5644c5726b50228884699b54ed59f906c4ff79/diff/cei
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/881cd097b8285eab427f138a7a5644c5726b50228884699b54ed59f906c4ff79/diff/cei
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/8a5aa05b62ebc949b91c3cc7f97e7cb2af664beddf946bc480ecc9ed3ddd231c/diff/hu
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8a5aa05b62ebc949b91c3cc7f97e7cb2af664beddf946bc480ecc9ed3ddd231c/diff/hu
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b26d0dfd0c1c4ff678551d8d0e6f00646816726bf558e199d60297b2aaf5e21/diff/dd
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b26d0dfd0c1c4ff678551d8d0e6f00646816726bf558e199d60297b2aaf5e21/diff/de
http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/d
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/d
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0945c6870d01f657d32a39a4312781f898b92d669cc73e64608d2b4e11ec0b97/diff/ar
http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/d
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/d
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/d
https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a2dd366044cbc04c04ff3615133afe3319254354f3895158b8281ccf77f4408/diff/e2c'
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/d
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a2dd366044cbc04c04ff3615133afe3319254354f3895158b8281ccf77f4408/diff/e2c'
/ https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/8d58d04c32042a241d38391c79e76173de9a8df4642529ebc8217152671b2678/diff/lu
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8d58d04c32042a241d38391c79e76173de9a8df4642529ebc8217152671b2678/diff/lu
http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bi
http://127.0.0.1	['sample_C1.zip', 'NVMe/docker/overlay2/8d9b5686369bb8ee5a95c7368566fafb0cbff4bab0618748e47fa348a9e06007/diff/ho
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8d9b5686369bb8ee5a95c7368566fafb0cbff4bab0618748e47fa348a9e06007/diff/ho
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bi
http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bi
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/lil
http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/lil
http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0c0f56417f5873b1f5996a08dcdad0d3ddb0e513ff0cb507855a65f17abada84/diff/se
and the second sec	n in the second s

### Figure 31: C1 Infoleak URLs (Black Duck)

Component	Version	Latest version	CVE	Matching type	CVSS CVE publication date	Object compilation dat	e Object	Object full path Object
lask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/docker/overlay2/7087348acaf6 c110215
Flask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/docker/overlay2/b34e88f83ef{c110215
lask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/docker/overlay2/b529d29db86c110215
Flask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/registry/docker/docker/registic110215
Flask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/registry/docker/docker/registic110215
Flask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0 c110215
Flask	1.1.1	2.2.2	CVE-2023-30861	Exact match	3.7 2023-05-04T08:43:23Z	2021-08-25T11:41:46Z	flask.app.pyc	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0 c110215
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:52Z	bash	sample_C1.zip:NVMe/docker/overlay2/0a9d8212dfe 79151d
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/docker/overlay2/8b92d275d3179151d
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/registry/docker/docker/registi79151d
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/ssd/1/swm/VER/10374.VswdB 79151d
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match	10 2014-09-28T19:55:00Z	2021-02-23T12:03:23Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/10SWV2.216a38460
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match	10 2014-09-28T19:55:00Z	2021-01-26T16:32:01Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0(3712a04
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:52Z	bash	sample_C1.zip:NVMe/docker/overlay2/0a9d8212dfe 79151d
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/docker/overlay2/8b92d275d3179151d
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/registry/docker/docker/registi 79151d
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match	10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/ssd/1/swm/VER/10374.VswdB 79151d
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match	10 2014-09-28T19:55:00Z	2021-02-23T12:03:23Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/10SWV2.216a38460
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match	10 2014-09-28T19:55:00Z	2021-01-26T16:32:01Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0/3712a04
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match	10 2014-09-25T01:55:00Z	2019-02-21T10:51:52Z	bash	sample_C1.zip:NVMe/docker/overlay2/0a9d8212dfe 79151d
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match	10 2014-09-25T01:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/docker/overlay2/8b92d275d3179151d
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match	10 2014-09-25T01:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/registry/docker/docker/registi 79151d
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match	10 2014-09-25T01:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/ssd/1/swm/VER/10374.VswdB 79151d
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match	10 2014-09-25T01:55:00Z	2021-02-23T12:03:23Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/10SWV2.216a38460
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match	10 2014-09-25T01:55:00Z	2021-01-26T16:32:01Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0 3712a0
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match	10 2014-09-30T10:55:00Z	2019-02-21T10:51:52Z	bash	sample_C1.zip:NVMe/docker/overlay2/0a9d8212dfe 79151d
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match	10 2014-09-30T10:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/docker/overlay2/8b92d275d3179151d
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match	10 2014-09-30T10:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/registry/docker/docker/registi 79151d
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match	10 2014-09-30T10:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/ssd/1/swm/VER/10374.VswdB 79151d
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match	10 2014-09-30T10:55:00Z	2021-02-23T12:03:23Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/10SWV2.216a38460
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match	10 2014-09-30T10:55:00Z	2021-01-26T16:32:01Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0(3712a04
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match	10 2014-09-27T22:55:00Z	2019-02-21T10:51:52Z	bash	sample_C1.zip:NVMe/docker/overlay2/0a9d8212dfe 79151d
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match	10 2014-09-27T22:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/docker/overlay2/8b92d275d3179151d
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match	10 2014-09-27T22:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/registry/docker/docker/registi 79151d
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match	10 2014-09-27T22:55:00Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/ssd/1/swm/VER/10374.VswdB 79151d
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match	10 2014-09-27T22:55:00Z	2021-02-23T12:03:23Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/10SWV2.216a38460
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match	10 2014-09-27T22:55:00Z	2021-01-26T16:32:01Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0(3712a04
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match	5.9 2017-09-13T08:53:25Z	2019-02-21T10:51:52Z	bash	sample_C1.zip:NVMe/docker/overlay2/0a9d8212dfe 79151d
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match	5.9 2017-09-13T08:53:25Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/docker/overlay2/8b92d275d3179151d
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match	5.9 2017-09-13T08:53:25Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/registry/docker/docker/registr 79151d
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match	5.9 2017-09-13T08:53:25Z	2019-02-21T10:51:53Z	bash	sample_C1.zip:NVMe/ssd/1/swm/VER/10374.VswdB 79151d
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match	5.9 2017-09-13T08:53:25Z	2021-02-23T12:03:23Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/10SWV2.216a38460
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match	5.9 2017-09-13T08:53:25Z	2021-01-26T16:32:01Z	bash	sample_C1.zip:NVMe/ssd/1/version/VER/V2.21.01.0 3712a0
		rabilities	+				1	(a) A start and the start of a start start of the star

Figure 32: C1 CVEs (Black Duck)



# Sample C1 Code Sentry Scan Report Excerpts

Figure 33: C1 Scan Overview (Code Sentry)

#### GRAMMATECH

#### <sup>I</sup>CODESentry<sup>-</sup>

### N-Day Findings Summary

Name	Version	Vendor	Security Score	Number of Vulnerabilities	Path
abseil	0~20200225.2	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ d6b78809c7d314892e2e768caf6c36 b61160cc0fc3f6904118b2eba9e08a c97a/diff/lib/libadlik_serving.so
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ 244d5830ec9dad40a01c 0c38b85bd20bd5c85fa08c6fe5ff1d 2d25e852fdc2b4/diff/ordinaryus erhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ 244d5830ec9dad40a01c 0c38b85bd20bd5c85fa08c6fe5ff1d 2d25e852fdc2b4/diff/ordinaryus erhome/setfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ 2af8e33e510b55ae4eda6cf1b8941b 01e12e990961e366011a 7da4ece862280b/diff/ordinaryus erhome/geffacl
aci	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ 2af8e33e510b55ae4eda6cf1b8941b 01e12e990961e366011a 7da4ece862280b/diff/ordinaryus erhome/setfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ 67c1e0517f180b47a8c db284e1d0ab0a1ee20a2 87d890d179406d4328f8d892/diff/ ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample C1.zip/NVMe/docker/overlay2/ 9c7ba484e32250c008b7 10c0380c8e7cc76d0938 ea67279dabd0a0bfdfa1be1/diff/ ordinaryuserhome/geffacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ 9c7ba484e32250c008b7 10c0380c8e7cc76d0938 ea67279daba0a0btidfa1be1/diff/ ordinaryuserhome/setfaci
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1.zip/NVMe/docker/overlay2/ a4ab53eb37cd01459dde f42225a56e60020d4dc2 04a486aeded319fc8505171b/diff/ ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_ C1 zip/NVMe/docker/overlay2/ a/b4411748/dca161986 724cec4ab9db39d21b3b 11569637220e6da84c576a3/diff/ ordinaryuserhome/setfacl

www.grammatech.com

Page 2 / 950

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 34: C1 N-day findings (Code Sentry)



## <sup>I</sup>CODESentry<sup>-</sup>

**N-Day Findings** 

Findings for sample\_C1.zip

Scan Depth: Shallow MD5: d05541efa7055b14f74ce217da685191 Number of Vulnerabilities: 12303

linux [unspecified] 2.4.20-wolk4.14-fullkernel

Match Level: Low Security Score: 0 Path: NG rescans/C1 rescan/sample\_C1.zlp/NVMe/docker/overlay2/ 5292f87836e697470edcfe706a889df0ae2d15abe3ff91f97df7b24fa6395228/dlff/pcs.exe Component ID: 48373a2d-9959-47f9-a5ca-7c707aa4930d

Score Distribution: 🖗 Unassigned: 0 🗢 None: 26 0 Low: 262 🔺 Medium: 799 🚦 High: 456 🔮 Critical: 32

Sev	verity	Score	CVSS Version	Vulnerability ID	Description
00	Critical	10	2.0	24041	Linux Kernel rndis.c OID_GEN_SUPPORTED_LIST Memory Corr
8	Critical	10	2.0	48120	Linux Kernel video4linux (V4L) uvcvideo uvc_driver.c uv
<b>Ø</b> (	Critical	10	2.0	49957	Linux Kernel libertas Subsystem drivers/net/wireless/li
<b>Ø</b> (	Critical	10	2.0	51253	Linux Kernel sctp net/sctp/sm_statefuns.c FWD-TSN Chunk
<b>Ø</b> (	Critical	10	2.0	61788	Linux Kernel drivers/net/e1000e/netdev.c Ethernet Frame
<b>Ø</b> (	Critical	10	2.0	67243	Linux Kernel fs/nfsd/nfs4xdr.c NFS XDR Compound Request
<b>Ø</b> (	Critical	10	2.0	67896	Linux Kernel L2TP drivers/net/pppol2tp.c pppol2tp_xmit
<b>0</b> (	Critical	10	2.0	74679	Linux Kernel Bluetooth net/bluetooth/l2cap_core.c l2cap
<b>0</b> (	Critical	10	2.0	93755	Linux Kernel drivers/target/iscsi/iscsi_target_paramete
00	Critical	10	2.0	104658	Linux Kernel /netfilter/nf_conntrack_proto_dccp.c DCCP
<b>0</b> (	Critical	10	2.0	107650	Linux Kernel hugetb_entry Callback Handling Unspecifie
<b>0</b> (	Critical	10	2.0	122243	Linux Kernel OZWPAN USB Host Controller Driver ozhcd.c
<b>0</b> (	Critical	10	2.0	122244	Linux Kernel OZWPAN USB Host Controller Driver ozusbsvc
<b>Ø</b> (	Critical	10	2.0	137359	Linux Kernel drivers/usb/usbip/usbip_common.c usbip_rec
<b>Ø</b> (	Critical	10	2.0	148130	Linux Kernel nf_ct_frag6_queue() Function IPv6 Packet D
<b>Ø</b> (	Critical	10	2.0	156288	Linux Kernel drivers/net/macsec.c macsec_start_xmit() F
00	Critical	10	2.0	179535	Linux Kernel drivers/char/random.c crng_ready() Functio
00	Critical	9.8	3.0	205886	Linux Kernel sound/soc/codecs/wcd9335.c wcd9335_codec_e
<b>Ø</b> (	Critical	9.8	3.0	212917	Linux Kernel drivers/net/ethernet/hisilicon/hns3/hns3pf
<b>Ø</b> (	Critical	9.8	3.0	212918	Linux Kernel drivers/net/wireless/ath/ath6kl/wmi.c ath6
00	Critical	9.8	3.0	212920	Linux Kernel fs/cifs/smb2pdu.c SMB2_write() Function re
<b>Ø</b> (	Critical	9.8	3.0	212921	Linux Kernel fs/cifs/smb2pdu.c SMB2_read() Function req
00	Critical	9.8	3.0	212942	Linux Kernel drivers/net/wireless/rsi/rsi_91x_mac80211
00	Critical	9.8	3.0	212953	Linux Kernel kernel/trace/trace.c allocate_trace_buffer
<b>0</b> (	Critical	9.8	3.0	252698	Linux Kernel fs/f2fs/node.c get_next_net_page() Functio
00	Critical	9.8	3.0	262402	Linux Kernel drivers/net/usb/hso.c hso_free_net_device(
00	Critical	9.8	3.0	274228	Linux Kernel fs/nfsd/nfs4xdr.c nfsd4_decode_bitmap4() F

www.grammatech.com

Page 156 / 950

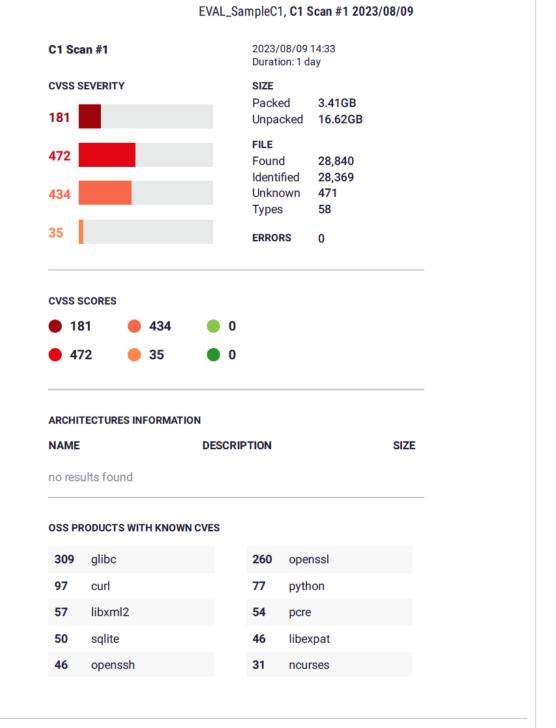
CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 35: C1 Vulnerabilities (mapped to CVEs in the report) (Code Sentry)

# Sample C1 Jarvis Scan Report Excerpts

#### **Summary Report**

💄 Charles.Begian



BlackBerry.

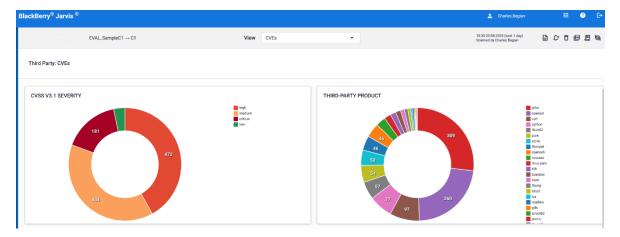
JARVIS

Created: 2023-04-

Figure 36: C1 Scan Overview (Jarvis)

EVAL_DempireC1 -= C1		View Cassified Drings +		10 Million Barrandia
matten Laskage: Classified Strings (BETA)				
NG CATEGORY	■ *far ■ *far	ntre salage Atmosfer Park	вляно тиче	■ Strack (spack) ● arc Mark ● Prof
		7		<ul> <li>The second sec</li></ul>
Jampie C1 dia WVMa Vesiany doday duoter Vesiany / 2 biobs/st a255 W1 V15HotoRbd1et7248da2a4c28b0200-165	dites 195	CATEGORY Ministric Lating	100	RAL STIME Intel from the State of the State
REINFO THE MICH Tarry C. C. SUNDALLY IN THE THE THE OWNER OF THE	Source file path	Information Lealinge	tas liptilitas lime, if code institutioning instability of target common harder. In Charget de Harder h	/ stall get that how, if cade instrum include into Dimension much hardle. So Diargo Antoi
REING - REERS Jamp G. (1990). Angley state state injury (1994). WEIGHT - REISER / REISERS/ REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS Jamp G. (1990). Angley state state angle (1990). REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS - REISERS	Source file path	Information Leakage	r anna an tha ann a' feadairteann feadairtean Darais connach an der SinDarais den stader. 1 de lighte a finn a feadairteann feadairtea Charais connach an der Beatabhadh sharis an der i	/ zie figt fice. Vers. (Kooke institent include imm?) was a common hander. Se Changelebreit Jase figt fice. Vers. (Kooke institut include imm?) was a common hander. Reestablief Disks
	Dourse file parts General file parts General file parts	Monation Lealage Monation Lealage Monation Lealage	constant factoria fina de la constante intervienda de la constante de la constante de la constante de la const Inter la ple de la constante de la decla de la constante d Inter la ple de la constante de	i de ligt fest im "Frankrinn in du de im 73 mes i comon hander la Chargoland i de ligt fest im "Frankrinn in du de im 74 mes i como hander Reseal du Dista i de ligt fest im "Frankring gelein verligtet ges i fest inden figer, gy
NA MIGH STA MIN MINING CONTRACTOR AND ADDRESS AND ADDRESS ADDRESS ADDRESS ADDRESS MINING CONTRACTOR ADDRESS ADDRES	Source Trapel	Hefermation Lealinge Information Lealinge Information Lealinge Hefermation Lealinge	comparison of the second secon	. Antibipitas Tem, Bradomenimo Teccale en Orane como la esta de Sel application (antibipitas Tem, Bradul noi non la como la como tecnario de altre Teccale) de Sel Antibipitas Tem, Bradul noi non pieto no aplica y en Bradul Antipita (antibipitas Tem, Bradul no pieto no pieto non De Studient que Antibipitas Tem, Bradul no pieto non De Studient que
AL 60-1-AL AD Jump (1, pp 4)-AL AD Jump (2, pp 4)-AL AD	Sourcelle gan Sourcelle gan Sourcelle gan Sourcelle gan Sourcelle gan	Memotor Ladage Manatas Ladage Menation Ladage Memotor Ladage Memotor Ladage	, con light con the fill contains the clock with the Contain terms in the Contain terms of the Containt terms of th	An high free here, if cash in a low of a similar to the second model in the Society of the Socie
As and a start and an and a start and a st	Romen Kin gan Kanan Kin gan Kanan Kin gan Konan Kin gan Kanan Kin gan	Memotor Ladage Memotor Ladage Memotor Ladage Memotor Ladage Memotor Ladage	In the first term in the data many includes the Constant of the sector multi-back the Constant of the sector of th	A sala fata har, fi sala har kun ku sha ma Sala sala sala sala sala sala sala sal
NA MIN - INF AMD MIN - INF AMD MIN - INF AMD	Sourch yan Sourch yan Sourch yan Sourch yan Sourch yan Sourch yan	Menetini Lakinge Menetini Lakinge Menetini Lakinge Menetini Lakinge Menetini Lakinge Menetini Lakinge	y par by takes in the Andreas in the Machine in the Machine Carlow Summarian Barbiel Carlow particular to the Andreas in the Andreas intervention intervention in the Andreas interventi	<ul> <li>A set of the law of</li></ul>
	Searchape Searchape Searchape Searchape Searchape Searchape Searchape	Monator Lakage Kristenia Lakage Monator Lakage Kristenia Lakage Monator Lakage Monator Lakage	Conference on the conference of the conference o	A star by Easte They Takes The series in the stark time 12 were sub-reserved where the Sectory and annual Takes by Easte They Takes The Tak
NA MIN - NA MIN Mang C, José Managoro, Barra Mang C,	Suchape Suchape Suchape Suchape Suchape Suchape Suchape	Maneso Calago Maneso Calago Maneso Calago Maneso Calago Maneso Calago Maneso Calago Maneso Calago	tes for tas har, final densities for addes into a Caracterizen Facilitado Carage abande abade     respetations (Carabiterizen in Saladinis Caracterizen Facilitado Faciativa Facilitado Facilitado Facilitado Facilitado Facilitado Faci	Analytic has hur functioned in the second of the second or the second or the second of the seco
	Sundaya Kanalaya Kanalaya Sundaya Kanalaya Kanalaya Kanalaya	Mananciang Kinang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang	geo get taak han / taaka han noo kuda kina Giraa samana ka da bid da gedi ada saka aka gaa get taak han / taaka han ya kuda kina ya kuda kina gaa get taaka han / taaka hang kuda kina ya	And Self has have, if the data has not increasive to the data water of the second self-self-sequences of the second second self-self-sequences of the second s
	Auchteel Auchteel Auchteel Auchteel Auchteel Auchteel Auchteel Auchteel Auchteel Auchteel Auchteel	Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa	geographics have function in back in the Green larmore in back (%) despite the back     set to be the function of the set of th	A star by Each Inte, The Cale The Inter Nation The Street
AL MAY-INT AMIN MARK STATES AND	Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya Sundaya	Mananciang Kinang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang	geo get taak han / taaka han noo kuda kina Giraa samana ka da bid da gedi ada saka aka gaa get taak han / taaka han ya kuda kina ya kuda kina gaa get taaka han / taaka hang kuda kina ya	And Self has have, if the data has not increasive to 10 decay assessments about the Self-Decay advances on the self-self-self-self-self-self-self-self-
	Suchap Suchap Indexp Suchap Suchap Suchap Suchap Suchap Suchap Suchap	Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa Manano Langa	geographics have function in back in the Green larmore in back (%) despite the back     set to be the function of the set of th	A star by Each Inte, The Cale The Inter Instruction To Descent services the descent Scherge allowed The Inter In
AL MOL ALL MATH THE MOL ALL MATH MILES AND	Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat Auctopat	Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang	tes byte ben / testere in backen of teste some in testere in tes	And Ref Landon, T. San Shen Shen Yorkshow TC and a second se
AL MON - FLA MON THE MON - THE MON	Sunkapi Sunkapi Sunkapi Sunkapi Sunkapi Sunkapi Sunkapi Sunkapi Sunkapi Sunkapi	Mananciang Annua Cang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang	geographics has / fuels has / fuels has has had a hard Care spanners had a hord beginned and the fuel of the spanners had a hord beginned and the fuel of the spanners had a hord beginned and the fuel of the fuel hard base of the fuel har	Academic Section 2014, Se
	Suckapi Auckapi Auckapi Auckapi Auckapi Auckapi Auckapi Auckapi Auckapi Auckapi Auckapi Auckapi	Mananciang Annen Lang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang Mananciang	manufactures in Society and Society a	Academic Section 1. The Section 1. Sect

### Figure 37: C1 Information Leakage (Jarvis)





rvis <sup>®</sup>										
Charles.Begian@ ▼	EVAL_Sa	mpleC1 -								
<b>≑</b> NAME	¢ DATE	¢ CRITICAL	\$ HIGH	¢ MEDIUM	\$ LOW		♦ UNPACKED SIZE	IDENTIFIED	\$ FOUND	\$ TYPES
. <u>C1</u>	2023/08/09	181	472	434	35	3.41GB	16.62GB	28369	28840	58
	\$ NAME	¢ NAME	¢NAME ¢DATE ¢CRITICAL	¢ NAME ¢ DATE ¢ CRITICAL ¢ HIGH	¢NAME ¢DATE ¢CRITICAL ¢HIGH ¢MEDIUM	¢NAME ¢DATE ¢CRITICAL ¢HIGH ¢MEDIUM ¢LOW	¢ NAME ¢ DATE ¢ CRITICAL ¢ HIGH ¢ MEDIUM ¢ LOW ¢ PACKED SIZE	¢ NAME ¢ DATE ¢ CRITICAL ¢ HIGH ¢ MEDIUM ¢ LOW ¢ PACKED SIZE ¢ UNPACKED SIZE	¢ NAME ¢ DATE ¢ CRITICAL ¢ HIGH ¢ MEDIUM ¢ LOW ¢ PACKED SIZE ¢ UNPACKED SIZE ¢ IDENTIFIED	¢ NAME ¢ DATE ¢ CRITICAL ¢ HIGH ¢ MEDIUM ¢ LOW ¢ PACKED SIZE ¢ UNPACKED SIZE ¢ IDENTIFIED ¢ FOUND

Figure 39: CVE Summary by Severity (Jarvis)

A	В	C	D	E	F	G	Н	1	J	K	L	M	N
@timestamp	extensi	on file_info.SHA3-512	file_info.file_name	file_info.file_path	file_info.ff	ile_info.parent_path	file_info.relative_path	file_info.timestamp	has_expi	r issuer.common_name	issuer.co	u issuer.e	m issue
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/7e2d62	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	stecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/bee6ab	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/d68592	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		0 5489864cd9adee5c2584f4c4d8bd87a6433	8 beego.ort	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip/NVMe/registry	home/webmnt/config/beego.c	2023-08-09T14:34:37.804022	FALSE	null	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/1fab96	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/8aa032	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		0 5489864cd9adee5c2584f4c4d8bd87a6433	server.ort	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/8d9b56	2023-08-09T14:34:37.804022	FALSE	null	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/937731	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		0 5489864cd9adee5c2584f4c4d8bd87a6433	8 beego.ort	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/8d9b56	2023-08-09T14:34:37.804022	FALSE	null	CN	null	null
2023-08-09T14:34:37		0 5489864cd9adee5c2584f4c4d8bd87a6433	server.ort	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip/NVMe/registry	home/webmnt/config/server.c	2023-08-09T14:34:37.804022	FALSE	null	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/0dc849	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/4230f8	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
2023-08-09T14:34:37		4 470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1/	sample_C1.zip	NVMe/docker/overlay2/b29328	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
> c1_ce	rtificate	es +					:		_				

### Figure 40: C1 Certificates report (Jarvis)

Α	В	с	DE	F	G	H I	J	К	L M	N	0	P	Q	R	S	т
ffected_o	ertain	componer cv	e.cvss.v cve.cvss.v2.base_severity	cve.cvss.v2.estimate	ed cve.cvss.v2.vector	cve.cvss.v cve.cvss.v	cve.cvss	v cve.cvss.v30.vector	cve.cvss.v cve.cvss.v	cve.cvss.	v cve.cvss.	v cve.desci	ri cve.name	cve.nvd_info.published c	ve.nvd_info.pu	cve.nvd_info.up
1.0.2, 1.0.	TRUE	libcrypto	5 medium	FALSE	AV:N/AC:L/Au:N/C:P/I:N/A:N	5.3 medium	TRUE	CVSS:3.0/AV:N/AC:L/P	5.3 medium	FALSE	CVSS:3.1	There is a	CVE-2019-1551	1,575,656,100	12/6/2019	1,650,382,56
1.1.1, 1.1	TRUE	libcrypto	7.8 high	TRUE	AV:N/AC:L/Au:N/C:N/I:N/A:C	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/P	7.5 high	FALSE	CVSS:3.1	AV:N/AC:	CVE-2022-4450	1,675,887,300	2/8/2023	1,677,251,70
1.0.2, 1.0.	TRUE	libcrypto	5.4 medium	TRUE	AV:N/AC:H/Au:N/C:C/I:N/A:N	5.9 medium	TRUE	CVSS:3.0/AV:N/AC:H/I	5.9 medium	FALSE	CVSS:3.1/	Atiming	ECVE-2022-4304	1,675,887,300	2/8/2023	1,677,258,78
1.0.2, 1.0.	TRUE	libcrypto	4.3 medium	FALSE	AV:N/AC:M/Au:N/C:N/I:N/A:P	5.9 medium	TRUE	CVSS:3.0/AV:N/AC:H/I	5.9 medium	FALSE	CVSS:3.1	AV:N/AC:	H CVE-2021-23841	1,613,495,700	2/16/2021	1,673,282,46
8.1.0	TRUE	libcurl	7.8 high	TRUE	AV:N/AC:L/Au:N/C:C/I:N/A:N	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/P	7.5 high	FALSE	CVSS:3.1	A use aft	e CVE-2023-28319	1,685,135,700	5/26/2023	1,686,298,50
7.33.0, 7.	TRUE	libcurl	5 medium	FALSE	AV:N/AC:L/Au:N/C:N/I:N/A:P	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/P	7.5 high	FALSE	CVSS:3.1	libcurl-us	ii CVE-2021-22926	1,628,198,100	8/5/2021	1,672,942,92
7.20.0, 7.	TRUE	libcurl	4.6 medium	FALSE	AV:L/AC:L/Au:N/C:P/I:P/A:P	7.8 high	TRUE	CVSS:3.0/AV:L/AC:L/PI	7.8 high	FALSE	CVSS:3.1	curl 7.20.	0 CVE-2020-8177	1,607,976,900	12/14/2020	1,655,491,50
7.20.0, 7.	TRUE	curl	4.6 medium	FALSE	AV:L/AC:L/Au:N/C:P/I:P/A:P	7.8 high	TRUE	CVSS:3.0/AV:L/AC:L/PI	7.8 high	FALSE	CVSS:3.1	curl 7.20.	0 CVE-2020-8177	1,607,976,900	12/14/2020	1,655,491,50
= 7.73.0	TRUE	libcurl	4.3 medium	FALSE	AV:N/AC:M/Au:N/C:P/I:N/A:N	3.7 low	TRUE	CVSS:3.0/AV:N/AC:H/I	3.7 low	FALSE	CVSS:3.1	A malicio	CVE-2020-8284	1,607,976,900	12/14/2020	1,652,475,42
7.20.0, 7.	TRUE	libcurl	5 medium	FALSE	AV:N/AC:L/Au:N/C:P/I:N/A:N	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/P	7.5 high	FALSE	CVSS:3.1	A user ca	r CVE-2021-22946	1,632,946,500	9/29/2021	1,672,943,04
7.65.0, 7.1	TRUE	libcurl	5 medium	FALSE	AV:N/AC:L/Au:N/C:P/I:N/A:N	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/P	7.5 high	FALSE	CVSS:3.1	An inform	n CVE-2022-27775	1,654,179,300	6/2/2022	1,672,942,08
7.87.0	TRUE	libcurl	5.4 medium	TRUE	AV:N/AC:H/Au:N/C:N/I:N/A:C	5.9 medium	TRUE	CVSS:3.0/AV:N/AC:H/I	5.9 medium	FALSE	CVSS:3.1	A use aft	e CVE-2022-43552	1,675,973,700	2/9/2023	1,679,980,50
7.83.1	TRUE	libcurl	5 medium	FALSE	AV:N/AC:L/Au:N/C:N/I:N/A:P	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/P	7.5 high	FALSE	CVSS:3.1	libcurl pr	c CVE-2022-27781	1,654,179,300	6/2/2022	1,672,941,24
2.26	TRUE	libpthrea	5 medium	FALSE	AV:N/AC:L/Au:N/C:P/I:N/A:N	5.3 medium	TRUE	CVSS:3.0/AV:N/AC:L/P	5.3 medium	TRUE	CVSS:3.1)	Certain n	CVE-2010-3192	1,287,035,880	10/14/2010	1,585,668,72
= 2.31	TRUE	libpthrea	6.8 medium	FALSE	AV:N/AC:M/Au:N/C:P/I:P/A:P	8.1 high	TRUE	CVSS:3.0/AV:N/AC:H/I	8.1 high	FALSE	CVSS:3.1	An explo	CVE-2020-6096	1,585,779,300	4/1/2020	1,669,059,54
= 2.32	TRUE	libpthrea d libresolv libnsl libnss_ni s libcrypt libc librm librss_fil es libnss_fol mpat libutil	7.1 high	FALSE	AV:N/AC:M/AutN/C:N/I:N/A:C	5.9 medium	TRUE	CV55:3.0/AV:N/AC:4/i	5.9 medium	FALSE	CV55:3.1,	<sup>7</sup> , The iconv	r CVE-2019-25013	1,609,784,100	1/4/2021	1,667,504,2
- 6-26	THUE	nootn	7.x mg.	1 House	a nity accity accity control acc	5.5 Incuran	mor	erosaliy Aring Acing	5.5 116010111	TALUL	C + 33-3-4)	The room	CTC-2013-23013	2,000,704,200	47472022	4,001,004,4
	c1_c	ves 4								_						

## Figure 41: C1 CVEs (Jarvis)

L M	N 0 fo.f file_info.r	P	Q	R	5	T	U	V.	W	×	Y file info.r	z	AA	A8 AC	AD	AE	AF	AG	AH #	i aj ak	AL AM	AN	AO string	DA Q	AR
																			ile_into.stile_i	info.t file_info.t file_inf					
bit /sample_(ELF	RegularFil 2021-08-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_clog.exe		0	33,261	********		2023-08-0 REG	nwxr-xr-x appro		appro@opens		
bit /sample_(ELF	RegularFil 2021-08-2:		TRUE				FALSE		FALSE					/sample_(log.exe		0			0	2023-08-0 REG	rwar-xr-x hardlin		hardlink@ope		
bit /sample_tELF	RegularFil 2021-08-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0		******	0	2023-08-0: REG	nw-rr posix-				
	RCE RegularFil 2021-08-1:		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	7,077	0	2023-08-0 REG	rw-rr eay		eay@cryptsoft	.com	
	OW RegularFil 2018-05-0		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/ss		0		******	0	2023-08-0 REG	fill-ff	9 19701817			
	RCERegularFil 2021-08-1:		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	42,258	0	2023-08-0 REG	rw-rr daniel		-daniel@haxx.s		
bit /sample_(ELF	RegularFil 2018-05-0	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	66,800	0	2023-08-0! REG	nw-rr jsewar	d 19701817	- jseward@bzip	org	
bit /sample_(ELF	RegularFil 2021-07-1		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	60,168	0	2023-08-0 REG	rw-rr tz		-tz@iana.org		
cet/sample_(C_SOUR	RCERegularFil 2021-07-1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do	ocker/overl	0	33,188	1,316	0	2023-08-0 REG	rw-rr ekr	19701817	ekr@rtfm.com		
bit /sample_(ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/de	0 19701817-	0	33,188	129,368	0	2023-08-0 REG	rw-rr statyfs	19701817	statvfs@open	ish.com	
bit /sample_(ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do	0 19701817-	0	33,188	129,368	0	2023-08-0: REG	rw-rr statvfs	19701817	statvfs@open	ish.com	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do	0 19701817-	0	33,188	129,368	0	2023-08-0 REG	rw-rr statyfs	19701817	statvfs@open	sh.com	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817-	0	33,261	129,368	0	2023-08-0: REG	rwxr-xr-x statvfs	19701817	- statvfs@open	ish.com	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817-	0	33,261	129.368	0	2023-08-0 REG	nexr-xr-x statyfs	19701817	statyfs@open	sh.com	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817-	0	33.261	129.368	0	2023-08-0 REG	nexe-xr-x statyfs	19701817	statyfs@open	ish.com	
bit /sample (ELF	RegularFil 2021-01-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817.	0	33,261	129.368	0	2023-08-0*REG	rear-xr-x statyfs	19701817	statyfs@open	sh com	
bit /sample (ELF	RegularFil 2021-08-2		FALSE	TRUE	FALSE	FALSE	FALSE	/sample infoam/lil		1,101	33.024	614.520	1,101	2023-08-0" REG				tp256-cert-v01g	Ronanerh						
bit /sample (ELF	RegularFil 2021-08-2		FALSE	TRUE	FALSE	FALSE	FALSE	/sample (nfoam/lit		1,101	33.024	614,520	1,101	2023-08-0 REG				ert-v01@opens:							
bit /sample (ELF	RegularFil 2021-08-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample (NVMe/do		0	33,188	614,520	0	2023-08-0 REG				ert-v01@opens	
bit /sample (ELF	RegularFil 2021-08-2:		FALSE	TRUE	FALSE	FALSE	FALSE	/sample (nfoam/lit		1,101	33,024	614,520	1.101	2023-08-0 REG			aes256-gcm@i		sh.com						
			FALSE	TRUE	FALSE	FALSE	FALSE			1,101	33,024	614,520	1,101	2023-08-0 REG											
bit /sample_tELF	RegularFil 2021-08-2													/sample_infoam/lil										-etm@openssh	
bit /sample_(ELF	RegularFil 2021-08-2:		FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(nfoam/lib		1,101	33,024	614,520	1,101	2023-08-0: REG				l-etm@openssh							
bit /sample_(ELF	RegularFil 2021-08-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	614,520	0	2023-08-0: REG				1305@openssh.	
bit /sample_(ELF	RegularFil 2021-08-2:		FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(nfoam/lil		1,101	33,024	614,520	1,101	2023-08-0 REG				epenssh.com	8						
bit /sample_(ELF	RegularFil 2021-01-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	354,504	0	2023-08-0: REG	rw-rr- rijnda				
bit /sample_(ELF	RegularFil 2021-01-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(usr/bin/s		0	33,261	354,504	0	2023-08-0: REG	nexr-xr-x rijndae				
bit /sample_(ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_tusr/bin/s	± 19701817-	0	33,261	354,504	0	2023-08-0' REG	nwxr-xr-x rijndae	d-d 19701817	rijndael-cbc@	ysator.liu.se	
bit /sample_(ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_tusr/bin/s	19701817-	0	33,261	354,504	0	2023-08-0 REG	rwar-xr-x rijndae	H-cl 19701817	rijndael-cbc@	ysator.liu.se	
bit /sample_(ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_tusr/bin/s	a 19701817-	0	33,261	354,504	0	2023-08-0 REG	nwxr-xr-x nijndae	el-d 19701817	- rijndael-cbc@	ysator.liu.se	
bit /sample_(ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_tusr/bin/s	19701817-	0	33,261	354,504	0	2023-08-0: REG	rear-xr-x rijndae	H-d 19701817	rijndael-cbc@	ysator.liu.se	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817-	0	33,261	354,504	0	2023-08-0 REG	nexe-xr-x rijndae	d-cl 19701817	rijndael-cbc@	ysator.liu.se	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817-	0	33,261	354,504	0	2023-08-0" REG	rear-xr-x nindae	H-d 19701817	riindael-cbc@	vsator, liu.se	
bit /sample (ELF	RegularFil 2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	s 19701817-	0	33,261	354.504	0	2023-08-0 REG	nwar-xr-x rijndae	d-d 19701817	riindael-cbc@	vsator.liu.se	
bit /sample (ELF	RegularFil 2021-01-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample (usr/bin/s	19701817-	0	33,261	254 504	0	2023-08-0*REG	next-xr-x nindae				
	W RegularFil 2018-05-0		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample (NVMe/ss		0	33,188	REFERENCE	0	2023-08-07 REG	DW-ff S	19701817			
	W RegularFil 2018-05-0		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample (NVMe/ss		0		*****	0	2023-08-0 REG	nu-rr K	19701817			
	00\ RegularFil 2021-08-2!		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FAISE	TRUE	FALSE	FALSE	FALSE	/sample (NVMe/do		0	33,188	835	0	2023-08-07 REG	nw-rr kyle		kyle@mekyle.		
	00\ RegularFil 2021-08-2		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE	/sample (home/we)		1.103	33,256	835	1.103	2023-08-0 REG	rwar-x kyle		kyle@mekyle.		
dc/sample (XML														/sample (nfoam/sh											
	RegularFil 2021-08-0		FALSE	TRUE	FALSE	FALSE	FALSE			1,101	33,024	4,738	1,101	2023-08-0: REG	r bertie		bertietf@bwij								
de/sample_EXML	RegularFil 2021-08-0:		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	4,738		2023-08-0: REG			balazs.lengyel		
di/sample_(XML	RegularFil 2021-08-0		FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(nfoam/sh		1,101	33,024	4,738	1,101	2023-08-0' REG			- balazs.lengyel								
bit /sample_(ELF	RegularFil 2021-08-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	6,272	0	2023-08-0: REG			morgan@kern		
bit /sample_(ELF	RegularFil 2021-08-2		TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0	33,188	6,272	0	2023-08-0 REG	rw-rr morga		- morgan@kern		
bit /sample_tELF	RegularFil 2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(NVMe/do		0		6,272	0	2023-08-0: REG	nw-rr morga		- morgan@kern		
his farmals arer	man Jauril seas an ai	TRUT			TAITT		FAIRE	FAIFF	*****	-															

. . .

### Figure 42: C1 email addresses (Jarvis)

1	0	5

A	8	C	D	E	. F	G	н	L	JK	1	M	N	0	P.	Q
@timestamp	cracked_pw	file_info.SHA3-512	file_info.file_name	file_info.file_path	ile_info.ffil	e_info.parent_path	file_info.relative_path	file_info.timestam gid	homedir	passwo	rd realname	scan_id	shell	uid	username
2023-08-09T14:35:37.862472	NO PASSWORD	2e582677e49f3056e1	esysmanager_ping.htm	/sample_C1.zip/NVMe/registry/do	HTML /s	ample_C1.zip/NVMe/registry/docker/d	ocker/regpagefile/html/chinese/sysmanager_ping.htm	2023-08-09T14:35:3	0 /root		Linux User,	19701817-13e0-441	f-1/bin/sh		0 root
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	33 /var/www	•	www-data	19701817-13e0-441	f-i/bin/false	1	33 www-data
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	Eshadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	37 /var		Operator	19701817-13e0-441	f-i/bin/false	3	37 operator
2023-08-09T14:35:37.862472	NO PASSWORD	2e582677e49f3056e1	sysmanager_ping.htm	/sample_C1.zip/NVMe/registry/do	ITML /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg.pagefile/html/chinese/sysmanager_ping.htm	2023-08-09T14:35:3	1,000 /home/zte		Linux User	19701817-13e0-441	f-1/bin/sh	1,0	o zte
2023-08-09T14:35:37.862472		2e582677e49f3056e1	esysmanager_ping.htm	/sample_C1.zip/NVMe/registry/do	ITML /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg pagefile/html/chinese/sysmanager_ping.htm	2023-08-09T14:35:3	1,111 /home/sctp	х	Linux User	19701817-13e0-441	f-1/bin/nologin	1,1	L1 sctp
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	Shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	1 /usr/sbin		daemon	19701817-13e0-441	f-:/bin/false		1 daemon
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_CLzip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	2 /bin	•	bin	19701817-13e0-441	f-i/bin/false		2 bin
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	Shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample C1.zip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	65,534 /home		nobedy	19701817-13e0-441	f-i/bin/false	65,5	34 nebody
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	0 /root	•	root	19701817-13e0-441	f-i/bin/sh		0 root
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	Shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg etc/shadow	2023-08-09T14:34:3	3 /dev		sys	19701817-13e0-441	f-i/bin/false		3 sys
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_CLzip/NVMe/registry/docker/d	ocker/regietc/shadow	2023-08-09T14:34:3	100 /bin	•	sync	19701817-13e0-441	f-1/bin/sync		4 sync
2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do.	ASCII /s	ample_C1.zip/NVMe/registry/docker/d	ocker/reg.etc/shadow	2023-08-09T14:34:3	8 /var/speci/m	eil *	mail	19701817-13e0-441	f-i/bin/false		8 mail
c) c1 passwd-file	e-analysis	+					1	1				_			_

### Figure 43: C1 Password File Analysis (Jarvis)

file_info.extension		file_info.file_output	file_info.file_path	file_info.file_type	file_info.groups	file_info	fragment	netioc	path	query scheme		
. 5	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line term			RegularFile, Executabl	le REG		schemas.openxmlforma	e/officeDocument/2006/relationships/officeDocument*			mats.org/officeDocument/2006/r
-15	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line term	inatoi/sample_C1.zip/NVMe/regi	stry/dc JAVASCRIPT	RegularFile, Executabl	de REG		purlorg	/dc/elements/1.1	http	http://pui 19701817-13e0-44	
		ASCII text, with very long lines, with no line term			RegularFile, Executabl				t:/officeDocument/2006/custom-properties",Kn.CUST_P			mats.org/officeDocument/2005/o
	14.56b243b036f056b79c68.js				RegularFile, Executabl				t:/officeDocument/2006/relationships/theme*	http		mats.org/officeDocument/2006/r
	14.56b243b036f056b79c68.js				RegularFile, Executabl				ts/officeDocument/2006/relationships/worksheet*,*http		http://sch19701817-13e0-44	
-15	14.56b243b036f056b79c68.js				RegularFile, Executabl		","xmins:tablecoo":"h	t purl.org		http		1f-8512-df2fc0569de0
-35	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line term	inatoi/sample_C1.zip/NVMe/doc	ker/ow JAVASCRIPT	RegularFile, Executabl	ik REG		docs.oasis-open.org	/ns/office/1.2/meta/pkg	http	http://docs.oasis-open.org/	ns/office/1.2/meta/pkg
.exe	log.exe	ELF 64-bit LSB executable, x86-64, version 1 (GNU			RegularFile, Executabl			www.baidu.com		<none></none>	www.baidu.com	
axe. 0	log.exe	ELF 64-bit LSB executable, x86-64, version 1 (GNU			RegularFile, Executabl			www.baidu.com		<none></none>	www.baic 19701817-13e0-44	
	lmm_hf	ELF 64-bit LSB executable, x86-64, version 1 (GNU			RegularFile, Executabl			curl.haxx.se	/docs/http-cookies.html	https	https://cu19701817-13e0-44	
ttf	opensans.ttf	TrueType Font data, digitally signed, 19 tables, 1st			RegularFile, Font, Nor			www.ascendercorp.com				om/http://www.ascendercorp.o
.ttf	opensans.ttf	TrueType Font data, digitally signed, 19 tables, 1st			RegularFile, Font, Nor			www.verisign.com	/rpa	https	https://www.verisign.com/	
.ttf	opensans.ttf	TrueType Font data, digitally signed, 19 tables, 1st			RegularFile, Font, Nor			logo.verisign.com	/vsloge.gif0	http	http://logo.verisign.com/vs	
	typecheck-gcc.h	C source, ASCII text	/sample_C1.zip/NVMe/doc		RegularFile, Sourceco			curl.haxx.se	/docs/copyright.html	https	https://curl.haxx.se/docs/ci	
h	typecheck-gcc.h	C source, ASCII text	/sample_C1.zip/NVMe/regi		RegularFile, Sourcecor	d REG		curl.haxx.se	/docs/copyright.html	https	https://cu19701817-13e0-44	
7 .SVg	import_xml120.svg	SVG Scalable Vector Graphics image	/sample_C1.zip/NVMe/regi	stry/dc SVG	RegularFile, Image, No	OI REG		www.bohemiancoding.o		http	http://ww.19701817-13e0-44	
E .	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV	(Lep/sample_C1.zip/NVMe/dod	ker/oveELF	RegularFile, Executabl	le REG		curl.se	/libcurl/c/curl_easy_setopt.html	https	https://curl.se/libcurl/c/cur	
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV	(Lec/sample_C1.zip/NVMe/doc	ker/ov(ELF	RegularFile, Executabl	de REG		example.com	/file[1-100:10].txt	http	http://example.com/file[1-	100:10].txt
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV			RegularFile, Executabl			curl.se	/docs	https	https://curl.se/docs	
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV			RegularFile, Executabl			nowhereatall.example.c		http	http://noi19701817-13e0-44	
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV			RegularFile, Executabl			curl.se	/docs/ssloerts.html	https	https://curi.se/docs/ssicert	
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV			RegularFile, Executabl			curl.se	/docs/ssicerts.html	https	https://cu19701817-13e0-44	1f-8512-df2fc0569de0
1	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV			RegularFile, Executabl			www.notiocal.com		<none></none>	www.notiocal.com	
.md	readme.md	ASCII text	/sample_C1.zip/NVMe/doc		RegularFile, Documen			scripts.sil.org	/OFL	http	http://scripts.sil.org/OFL	
i .eot	iconfont.eot	Embedded OpenType (EOT), iconfont family	/sample_C1.zip/NVMe/doc		RegularFile, Font, Nor	n/ REG		fontello.com		http	http://fontello.com	
.yin	letf-netconf-with-defaults.y	ir XML 1.0 document text	/sample_C1.zip/NVMe/regi	stry/dc XML	RegularFile, Markup, 1	N REG		trustee.letf.org	/license-Info	http	http://tru 19701817-13e0-44	
_svg	Error.svg	SVG Scalable Vector Graphics image	/sample_C1.zip/NVMe/regi	stry/dc SVG	RegularFile, Image, No			sketchapp.com		https	https://sk 19701817-13e0-44	1f-8512-df2fc0569de0
js	vendor.b9bd44bbd3e0c69b9	CUTF-B Unicode text, with very long lines	/sample_C1.zip/NVMe/doc	ker/oveJAVASCRIPT	RegularFile, Executabl	le REG	/zh-CN/component/u	element.eleme.io	1	http	http://element.eleme.io/#	zh-CN/component/upload#yong
a, js	vendor.b9bd44bbd3e0c69b9	t UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/doc	ker/oveJAVASCRIPT	RegularFile, Executabl	de REG	/zh-CN/component/u	element.eleme.io	1	http	http://ele19701817-13e0-44	1f-8512-df2fc0569de0
1.js	main.2485230bcb7306882473	ASCII text, with very long lines, with no line term			RegularFile, Executabl	ile REG	Inchange-propagation	angular.io	/docs/ts/latest/api/common/index/NgFor-directive.ht	ml https	https://angular.io/docs/ts/l	atest/api/common/index/NgFor-
2 .txt	3rdpartylicenses.txt	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/doc	ker/oveTEXT_FILE	RegularFile, Text, Non	n/ REG		kossnocarp.mit-license.	ang	http	http://kossnocorp.mit-licen	se.org
.txt	3rdpartylicenses.txt	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/regi		RegularFile, Text, Non			kossnocorp.mit-license.		http	http://ko:19701817-13e0-44	
txt. 3	3rdpartylicenses.txt	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/regi		RegularFile, Text, Non			tidrlegal.com	/license/mit-license	https	https://tic19701817-13e0-44	
	webmnt	ELF 64-bit LSB executable, x86-64, version 1 (GNU			RegularFile, Executabl			beego.me	/docs/module/toolbox.md*>Toolbox <td>http</td> <td>http://bec19701817-13e0-44</td> <td></td>	http	http://bec19701817-13e0-44	
5	webmnt	ELF 64-bit LSB executable, x86-64, version 1 (GNU			RegularFile, Executabl	ile REG		beego.me	/docs/advantage/monitor.md*>Live	http	http://bei19701817-13e0-44	
7 .conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/regi		RegularFile, Configura	at REG		redis.io	/topics/client-side-caching	https	https://re 19701817-13e0-44	1f-8512-df2fc0569de0
i .conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/doc	ker/ow CONFIG	RegularFile, Configura	at REG		redis.lo	/topics/acl	https	https://redis.io/topics/acl	
.conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/doc	ker/oveCONFIG	RegularFile, Configura	at REG		redis.io	/topics/persistence	http	http://redis.io/topics/persit	tence
hoonf	redis.conf	ASCII text	/sample_C1.zip/NVMe/regi	stry/dc CONFIG	RegularFile, Configura	et REG		antirez.com	/post/redis-persistence-demystified.html	http	http://ant19701817-13e0-44	1f-8512-df2fc0569de0
Jhtml	demo_index.html	HTML document text	/sample_C1.zip/NVMe/doc	ker/ov(HTML	RegularFile, Documen	nt REG		img.alicdn.com	/tps/i4/TB1_oz6GVXXXXXFXpXXIDFnXXXXF4-64.ico	https	https://img.alicdn.com/tps/	4/TB1_026GVXXXAFXpXXUDFnIX
h	bn.h	C source text C source text C source text	/sample_C1.zip/NVMe/dod	ker/oveC_SOURCE	RegularFile, Sourcecor	d REG		magma.maths.usyd.edu	s/calc	http	http://magma.maths.usyd.e	du.au/calc
h	bn.h	C source text C source text C source text	/sample_C1.zip/NVMe/regi	stry/dcC_SOURCE	RegularFile, Sourcecor	d REG		magma.maths.usyd.edu	a/calc	http	http://ma 19701817-13e0-44	1f-8312-df2fc0569de0
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV	(Lec/sample_C1.zip/NVMe/doc	ker/oveELF	RegularFile, Executabl	de REG		curl.haxx.se	/libcurl/c/curl_easy_setopt.html	https	https://curl.haxx.se/libcurl/	c/curl_easy_setopt.html
	curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV	(Lec/sample_C1.zip/NVMe/regi	stry/dc ELF	RegularFile, Executabl	ile REG		curl.haxx.se	/libcurl/c/curl_easy_setopt.html	https	https://cu19701817-13e0-44	
	curi	ELF 64-bit LSB executable, x86-64, version 1 (SYSV	(Lep/sample_C1.zip/NVMe/doc	ker/ow ELF	RegularFile, Executabl	de REG		curl.haxx.se	/docs/ssicerts.html	https	https://curl.haxx.se/docs/st	
	weblmt	ELF 64-bit LSB executable, x86-64, version 1 (GNU	/Linus/sample_C1.zip/NVMe/doc	ker/ov(ELF	RegularFile, Executabl	de REG		schemas.openxmlforma	t:/officeDocument/2006/relationships	http	http://schemas.openxmlfor	mats.org/officeDocument/2005/
	weblmt	ELF 64-bit LSB executable, x86-64, version 1 (GNU			RegularFile, Executabl				t:/drawingml/2006/spreadsheetDrawing	http		mats.org/drawingml/2006/spread
	mathfast	EI C 64 hit I CD avan dable and 64 services 1 (Chill)	Dinis Isamela C1 ale BOHLe Isani	steaded DIE	BoudarCite Constabil			ourl arts are	Incombinecodebootmillessiningen	htto	hannelleur 10701017 1200 A	to be the destroy of the second

Figure 44: C1 Infoleak URL report (Jarvis)

	ST ~		Download ~	Upload
Overview	Bill of Materials Findings Scar	ns Files		
	Risk		Details	
	RISK			
	100 / 100		Operating Systems	
	0 10 35 6	65 100	Linux Kernel 4.9.115, Linux Kernel 4.19.31, Linux Kernel 4.19.82 and Linux Kernel 4.4.157	
			EreeRTOS 7.0.0 and FreeRTOS 8.2.3	
	Findings Detected		VxWorks Unknown	
	TOIL		Architectures	
	Software Components			
	3,200		Products Depending On This Artifact	
			August 2023 100	
			Created	
			charles.begian@ngc.com	
			August 30, 2023	
	Finding Exploit Intelligence		Remediation Guidance ①	
	Category	<i>l</i> ₹ Count		
	✓ No Known Exploits	43,416 findings	Guidance	
	Proof of Concept Exploit	02,049 findings	Address high risk component /NVMe/registry/docker/docker/reg /sha256	
	✤ Weaponized	① 70 findings	/c4/c4313c23b61a530de7f926d024acc5c9149b9509c1b7c108 /data/data~/sbin/chown	
	Reported in the Wild	① 21 findings	Address high risk component /NVMe/docker/overlay2 /1db9c1884a144a6c3e4cfea49f8cd6a78157a11e83290efb301b	
	Exploited By Threat Actors	① 11 findings	, /diff/ordinaryuserhome/ftpd	
			Address high risk component /NVMe/registry/docker/docker/reg /sha256	

# Sample C1 Finite State Platform Scan Report Excerpts

Figure 45; C1 Scan Overview (Finite State Platform)

C1 > TEST > Overview Bill of Materials Findings	Scans	Files					Download V Upload
Findings by Severity 46K findings • Low (10620) • Medium (34417) • High (460) • • Unknown (0)	Critical (3	8)		Category No Pro Vec Rep	Exploit Intelligence Known Exploits of of Concept Exploit aponized ported in the Wild ploited By Threat Actors		IF Count 43,416 findings • 2,049 findings • 70 findings • 21 findings • 11 findings
Iffitter      Q    Search findings		<b>0</b>	=↓ Risk		CVE	CWE	
CVE-2015-0235 - glibc-devel:2.17	Ó	Severity	<b>10</b> /10	Status	CVE-2015-0235	CWE-787	Found By Finite State Monitoring
CVE-2015-0235 - glibc:2.17	۵	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2015-0235 - glibc-devel:2.17	ම	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2015-0235 - glibc:2.17	ම	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2016-2108 - OpenSSL:0.9.8za		Critical	<b>9.7</b> /10		CVE-2016-2108	CWE-119	Finite State Monitoring
CVE-2022-1292 - OpenSSL:1.1.1	۵	Critical	<b>9.5</b> /10		CVE-2022-1292	CWE-78	Finite State Monitoring
CVE-2022-1292 - OpenSSL:1.1.1d	ම	Critical	<b>9.5</b> /10		CVE-2022-1292	CWE-78	Finite State Monitoring
-							

Figure 46: C1 Scan Findings (Finite State Platform)

D	E
category	subcategory
CREDENTIALS	PASSWD_USER_ACCOUNTS
CRYPTO_MATERIAL	PEM_CERTIFICATE_KEY
CRYPTO_MATERIAL	EXPIRED_CERTIFICATE
CRYPTO_MATERIAL	PEM_CERTIFICATE_EXPIRED
SAST_ANALYSIS	USE_AFTER_FREE
SAST_ANALYSIS	HEAP_BUFFER_OVERFLOW
SAST_ANALYSIS	DOUBLE_FREE
CONFIG_ISSUES	SSH_PERMIT_ROOT
SAST_ANALYSIS	UNCHECKED_RETURN_VALUE
CONFIG_ISSUES	SSH_MAX_RETRIES
SAST_ANALYSIS	EXPRESSION_ALWAYS_TRUE
SAST_ANALYSIS	INHERENTLY_DANGEROUS_FUNCTION
SAST_ANALYSIS	IMPROPER_LENGTH_HANDLING
SAST_ANALYSIS	INCORRECT_BEHAVIOR_ORDER
SAST_ANALYSIS	VERY_HIGH_CODE_COMPLEXITY
SAST_ANALYSIS	HIGH_CODE_COMPLEXITY
CREDENTIALS	SHADOW_HARD_CODED_PASSWORDS
CREDENTIALS	PASSWD_HARD_CODED_PASSWORDS
CRYPTO_MATERIAL	SSH_PRIVATE_KEY
CONFIG_ISSUES	SELINUX_DISABLED
CRYPTO_MATERIAL	SELF_SIGNED_CERT
SAST_ANALYSIS	VXWORKS_EXE_NO_PASSWORD
SAST_ANALYSIS	STACK_BUFFER_OVERFLOW
CRYPTO_MATERIAL	PKCS8_PRIVATE_KEY
CVE	KNOWN_VULNERABILITIES
> C1_TEST.	findings +

Figure 47: C1 Findings Categories (Finite State Platform)

Α	В	С	D	G	Н	
/ulnIdFromTool	riskScore	cvssV3Sco	cvssVectorString	affectedComponents	exploitCount	maxExploitMaturit
CVE-2020-1967	7.2	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.1d	2	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1d	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2g	1	poc
CVE-2016-8610	7.3	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.0.2g	1	poc
CVE-2019-3822	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.52.1	1	poc
CVE-2019-5436	7.3	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	cURL:7.52.1	1	poc
CVE-2016-8610	7.3	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	poc
CVE-2016-7054	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	2	poc
CVE-2016-6304	7.2	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2016-6305	7.2	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2017-3730	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	4	рос
CVE-2016-7054	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	2	рос
CVE-2017-3730	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	4	poc
CVE-2016-6305	7.2	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	poc
CVE-2016-8610	7.3	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	poc
CVE-2016-6304	7.2	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	poc
VE-2021-43527	7.3	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NSS:3.12.4	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2n	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2k	1	poc
CVE-2015-8778	8.4	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	1	poc
CVE-2015-8779	8.6	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	1	poc
CVE-2014-9402	7.4			glibc:2.18	3	poc
CVE-2014-9761	8.7	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	2	poc
CVE-2014-9984	8.5	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	2	poc
CVE-2015-7547	8.1	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	18	weaponized
CVE-2015-8779	8.6	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	1	poc
CVE-2014-9984	8.5		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	2	poc
CVE-2014-9761	8.7	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	2	poc
CVE-2015-7547	8.1	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18		weaponized
CVE-2015-8778	8.4	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc:2.18	1	poc
CVE-2014-9402	7.4			glibc:2.18	3	poc
CVE-2022-0435	7.2	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:4.19.82	2	poc
CVE-2019-11479	7.5	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.19.31	1	poc
VE-2019-10125	9.4	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:4.19.31	1	poc
VE-2019-11478	7.5	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.19.31	1	poc
VE-2019-11477	7.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.19.31		poc
CVE-2022-0435	7.2		CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:4.19.31		poc
CVE-2022-1292	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1k		poc
CVE-2018-20843	7.4		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	expat:2.2.6		poc
NE 2022 25226	0 7	0.0		ovpoti2 2 6		200

Figure 48: C1 CVE Exploitability (Finite State Platform)

# **APPENDIX D: CST SCAN REPORT EXCERPTS FOR SAMPLE C2**

Black Duck Binary Analysis Search	n and jump to group 소 Upload • ⓒ • 옫 charles.begian •
Analysis settings File content	
General	
Name	sample_C2.zip 🕑
Description	No description given 🗹
Version	No version given 🗹
Uploaded	2023-08-09 15:47 (5 days ago) by charles.begian
Last scanned	2023-08-09 16:06 (5 days ago)
BDBA engine version used for scanning	20230608
BDBA frontend version used for calculation	20230615 LATEST
Protect from data retention	
Notify on new vulnerabilities	
File properties	
File	▲ Replace
File available	No
SHA1	2b74179390ae29ff1e08d76d086eb33417dae1c8
Size	1.16 GB (original) / 3.88 GB (scanned)
Analysis ③ Remove	
Application type	Windows executable
Duration	16 minutes
Throughput ③	114.35 MB/s
BDSA database version ①	2023-08-14T11:59:50 STALE
NVD database version ③	2023-08-14T06:15:00 STALE
Component database version ①	2023-08-14T04:04:31
Native fingerprint version	2023-05-31T10:04:47
Dotnet fingerprint version	2023-05-31T04:12:23.653096
Cocoapods fingerprint version	2023-06-07T07:52:47.754010
Golang fingerprint version	2023-06-08T07:16:22.448950
Python fingerprint version	2023-06-12T01:47:49.220082
Low risk tolerance mode	No ©
Include historical vulnerabilities	Yes ©
	Figure 49: C2 Scan Overview (Black Duck)

# Sample C2 Black Duck Scan Report Excerpts

# sample\_C2.zip

### Vulnerability analysis verdict: VULNS / Information leakage: VERIFY

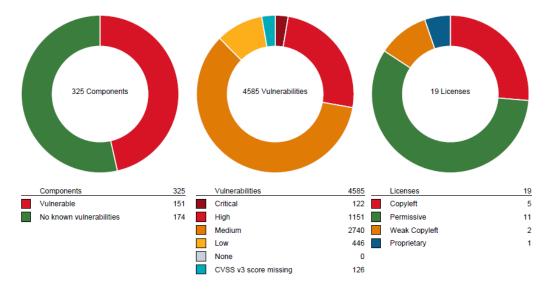


Figure 50: C2 Scan found 4585 Vulnerabilities (Black Duck)

### Details

Original filename	
SHA1 checksum	2b74179390ae29ff1e08d76d086eb33417dae1c8
Original file size	1157.58 MB

#### Infoleak

Asymmetric keys:	1251
AWS keys:	0
Custom pattern matches:	0
Emails:	6112
HTTP authentication:	0
Image metadata:	0
IP addresses:	4886
JSON web tokens:	3
MAC addresses:	41
OAuth tokens:	0
Passwords:	18
Shell history:	0
URLs:	7958
Twilio keys:	0
Google cloud keys:	0
Facebook access tokens:	0

Figure 51: C2 Information leaks (Black Duck)

A	B C	D	E	r	G	n	1		n.		m	N 0		Q	R	S		U		n	A	1	2	AA	AB	AC	A
Algorithm Bit		Private		d Content	User	Expires	Certificate	Attributes																			
RSA	1024 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY							SWc2/NVMe/do							kc1d0c809fa	a1e43c1c/o	diff/home/	weblmt/e	nv/python	2.7.12/lib/py	thon2.7	/test/bado	rt.pem"]	
RSA	1024 PEM	TRUE	FALSE	BEGIN PRIVATE KEY							SWc2/NVMe/ss																
RSA	2048 PEM	TRUE	FALSE	BEGIN PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/b31b611	a5362b78b6c	ff4809b701	.b3964dc8fi	d169467384	kc1d0c809fa	a1e43c1c/o	diff/home/	weblmt/to	ool/ssl.key	1				
RSA	2048 PEM	TRUE	FALSE	BEGIN PRIVATE KEY							SWc2/NVMe/ss																
RSA	2048 PEM	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/5e1c8c53	1b41de31fce	e5f3d2828f	0637bbfd18	388fe2068fi	7a4b0b02b4	4266ee9a/	diff/home	/webmnt/	backend/fi	les/ssl.key']				
RSA	2048 PEM	TRUE	FALSE	BEGIN PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/21412d8	o8dfb718436	3222f85172	f64721512	35b3fd1631	7fe1e2e374	44897c57/	diff/home,	/weblmt/ti	ool/ssl.key	1				
RSA	1024 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/21412d8	o8dfb718436	3222f85172	f64721512	35b3fd1631	7fe1e2e374	44897c57/	diff/home,	/weblmt/e	nv/python	2.7.12/lib/p	thon2.7	/test/bado	ert.pem']	
RSA	1024 PEM	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/4618ada	791fc0c31ab3	led9a94c7e	f524695db	c6c97ac72d	d8a242f3ca	289f9ee/	diff/tmp/_l	MEIn5omvi	b/app/files	s/ssl_key_art	/ipsec1.	key"]		
RSA	1024 PEM	TRUE	FALSE	BEGIN PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/5e1c8c53	1b41de31fce	e5f3d2828f	0637bbfd18	388fe2068fi	7a4b0b02b4	4266ee9a/	diff/home	/webmnt/	backend/w	ebmnt', 'ap	p/files/s	sl_key_crt/	psec1.ke	/1
RSA	0 PEM	TRUE	TRUE	BEGIN RSA PRIVATE KEY					['sample	e C2.zip', 'V	SWc2/NVMe/ss	d/weblmt u	tility/pytho	n2.7.12/lib/p	ython2.7/	test/keyce	rt.passwd.p	pem']									
RSA	0 PEM	TRUE	TRUE	BEGIN RSA PRIVATE KEY					['sample	e C2.zip', 'V	SWc2/NVMe/ss	d/weblmt_u	tility/pytho	n2.7.12/lib/g	ython2.7/	test/ssl ke	y.passwd.p	em')									
RSA	1024 PEM	TRUE	FALSE	BEGIN PRIVATE KEY					['sample	e C2.zip', 'V	SWc2/NVMe/do	cker/overla	/2/5e1c8c53	1b41de31fce	5f3d2828f	0637bbfd18	388fe2068fi	7a4b0b02b4	1266ee9a/	diff/home	/webmnt/	backend/fi	les/ipsec1.k	ey']			
RSA	0 PEM	TRUE	TRUE	BEGIN RSA PRIVATE KEY					['sample	e C2.zip', 'V	SWc2/NVMe/do	cker/overla	/2/b31b611	a5362b78b6c	ff4809b701	b3964dc8fi	169467384	kc1d0c809fa	a1e43c1c/u	diff/home/	weblmt/e	nv/ovthon	2.7.12/lib/ov	rthon2.7	/test/kevce	rt.oasswd	l.oe
RSA	1024 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY							SWc2/NVMe/do																
RSA	1024 PEM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/ss											41.5		0.11	1 1 - 1 -		1
RSA	2048 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY							SWc2/NVMe/do							63efff78a4	922761499	/diff/etc/s	sh/ssh ho	st rsa kevi	1				
RSA	1024 PFM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/do													rkages/r	wftodlih/te	st/kevrer	t ne
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do																
RSA	1024 PEM	TRUE	FALSE								SWc2/NVMe/do																
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do																
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do																
RSA	0 PEM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/do SWc2/NVMe/do																
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/ss							1000000016	icescient	anny nonney	wearinge	in pyrion	2.7.22/110/19/	110112-1	read an _0	1-ba2200	.pc
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/ss SWc2/NVMe/ss																
RSA	0 PEM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/do SWc2/NVMe/do							76102027	44007-57/	diff/homo	luchlet la	nulauthan	2 7 12/lib/m	thor? 7	(tort/kour	et exercise	d no
RSA	0 PEM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/do SWc2/NVMe/do																
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY						-	SWc2/NVMe/do SWc2/NVMe/do																the
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do SWc2/NVMe/do																-
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY																							
	1024 PEM										SWc2/NVMe/do																
RSA		TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do							ICTORCROALS	11643C1C/0	sitt/nome/	webimt/e	nv/pytnon	2.7.12/110/py	rtnon2.7	/test/ssi_k	y.pem j	
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/ss									i-tth		1.0	a 7 call:1 [		h .h		
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do																
RSA	1024 PEM	TRUE		BEGIN PRIVATE KEY							SWc2/NVMe/do															ey.pem']	
RSA	2048 PEM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/do							56cb00e31f	2eb2fd7/c	liff/mnt/fl	ash/PkiRoc	ot/vendor/	USER/2c26c5	ifff05f.ke	ey']		
RSA	1024 PEM	TRUE	FALSE								SWc2/NVMe/ss																
RSA	2048 PEM	TRUE		BEGIN RSA PRIVATE KEY							SWc2/NVMe/do																
RSA	1024 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY							5Wc2/NVMe/do								44897c57/	diff/home,	/weblmt/e	nv/python	2.7.12/lib/p	thon2.7	/test/wron	gcert.pen	ſ
RSA	1024 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY							SWc2/NVMe/ss																
RSA	1024 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY					['sample	e_C2.zip', 'V	SWc2/NVMe/do	ocker/overla	/2/b31b611	a5362b78b6c	ff4809b701	b3964dc8fi	169467384	kc1d0c809fa	a1e43c1c/o	diff/home/	weblmt/e	nv/python	2.7.12/lib/py	thon2.7	/test/wron	gcert.pem	1

Figure 52: C2 Asymmetric keys (Black Duck)

	B C	D	E	F	G	Н	1		K	L M	N	1 0	P	Q	R	S	T	U	V W	)	(	γ	Z	Щ	AB	AC	AD	Æ	AF	AG	AH	Al	AJ
Algorithm Bit			Encrypted		User	Expires																											
ECDSA	384 PEM	FALSE		BEGIN PUBLIC KEY						ip', 'VSWc2/N														-		-	Institutio	ns_ECC_Ro	CA_2015.0	rť]			
RSA	4096 PEM	FALSE		BEGIN PUBLIC KEY		2042-01-1				ip', 'VSWc2/N														_	_								
ECDSA	384 PEM	FALSE		BEGIN PUBLIC KEY		2038-01-1				ip', 'VSWc2/N																			yG4.ort]				
RSA	2048 PEM	FALSE		BEGIN PUBLIC KEY		2037-12-0				ip', 'VSWc2/N																	-						
RSA	4096 PEM	FALSE		BEGIN PUBLIC KEY		2042-01-1				ip', 'VSWc2/N																-							
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2025-05-1				ip', 'VSWc2/N																							
RSA	2048 PEM	FALSE		BEGIN PUBLIC KEY		2037-12-0				ip', 'VSWc2/N																							
RSA	2048 PEM	FALSE		BEGIN PUBLIC KEY		2029-12-3				ip', 'VSWc2/N																							
RSA	4096 PEM	FALSE		BEGIN PUBLIC KEY		2038-07-3				ip', 'VSWc2/N																							
ECDSA	384 PEM	FALSE		BEGIN PUBLIC KEY		2038-01-1				ip', 'VSWc2/N																							
RSA	2048 DER	FALSE	FALSE	BEGIN PUBLIC KEY	-	2019-03-04				ip', 'VSWc2/N																							
RSA	1024 PEM	FALSE		BEGIN PUBLIC KEY		2019-06-2				ip', 'VSWc2/N																							
RSA	1024 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2020-12-3				ip', 'VSWc2/N															ensurepip	/_bundler	1/pip-8.1	.1-py2.py3-	ione-any.w	hl', 'pip/_	vendor/req	iests/cace	st.pe
RSA	4096 PEM	FALSE		BEGIN PUBLIC KEY		2042-01-1				ip', 'VSWc2/N																							
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2025-05-1				ip', 'VSWc2/N																							
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2037-12-0				ip', 'VSWc2/N																							
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2029-12-3				ip', 'VSWc2/N																							
RSA	4096 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2038-07-3				ip', 'VSWc2/N																							
ECDSA	384 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2038-01-1				ip', 'VSWc2/N																							
RSA	2048 DER	FALSE	FALSE	BEGIN PUBLIC KEY	-	2019-03-0	TRUE {	"countryf ['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt_uti	lity/python2	.7.12/lib/py	thon2.7/ens	surepip/_	oundled/pip	-8.1.1-py2.p	y3-none-any	,whl', 'pi	p/_vendo	r/request	s/cacert.j	pem']									
RSA	1024 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2019-06-2	TRUE {	"locality*['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/webimt_uti	lity/python2	.7.12/lib/py	thon2.7/ens	surepip/_	oundled/pip	-8.1.1-py2.p	y3-none-any	, whi', 'pi	p/_vendo	r/request	s/cacert.j	pem']									
RSA	1024 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2020-12-3	TRUE {	"countryf ['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt_uti	lity/python2	.7.12/lib/py	thon2.7/ens	surepip/_	oundled/pip	-8.1.1-py2.p	y3-none-any	, whi', 'pi	p/_vendo	r/request	s/cacert.j	pem']									
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2025-05-1	TRUE {	"countryf ['s	ample_C2.z	ip', 'VSWc2/N	VMe/doc	ker/overlay3	1/19f93c84364	62c21857ec	5e20cbc3237	85e9c72d	bfef9c54237b	16ccf38594	798/diff/usr;	/share/ca	-certificat	tes/mozill	a/Baitim	ore_Cybe	rTrust_Ro	ot.ort']							
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2029-12-3	TRUE {	"countryf ['s	ample_C2.z	ip', 'VSWc2/N	VMe/doc	ker/overlay3	1/19f93c84364	62c21857ec	5e20cbc3237	85e9c72d	bfef9c54237t	16ccf38594	798/diff/usr;	/share/ca	-certificat	tes/mozill	а/сомоі	DO_Certi	fication_A	uthority.o	rť]						
RSA	4096 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2038-07-3	TRUE {	"countryf["s	ample_C2.z	ip', 'VSWc2/N	VMe/doc	ker/overlay3	1/19f93c84364	62c21857ec	5e20cbc3237	85e9c72d	bfef9c54237t	16ccf38594	798/diff/usr;	/share/ca	certificat	tes/mozill	a/Chamb	ers_of_C	ommerce <sub>.</sub>	Root - 2	["tro.800						
RSA	2048 DER	FALSE	FALSE	BEGIN PUBLIC KEY		2019-03-0-	TRUE {	"countryf ['s	ample_C2.z	ip', 'VSWc2/N	VMe/doc	ker/overlay2	1/19f93c84364	62c21857ec	5e20cbc3237	85e9c72d	bfef9c54237b	16ccf38594	798/diff/usr;	/share/ca	oertificat	es/mozill	a/GeoTru	ust_Globa	LCA_2.of	r]							
RSA	4096 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2042-01-1	TRUE {	"country" ['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01845-2P01	1-6_03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6_0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz', 'V.	2.19.00.01	B46-2P01-	5_030620	17.Vgcc1Ma	inCpu-7115	784-13923	6362', 'sbin)	lubancti", '	'cert
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2025-05-1	TRUE {	"country"["s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01846-2P01	1-6_03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6_0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz', 'V.	2.19.00.01	B46-2P01-	5_030620	17.Vgcc1Ma	inCpu-7115	784-13923	6362', 'sbin)	lubancti", '	'cert
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2037-12-0	TRUE {	"country"["s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01846-2P01	1-6_03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6_0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz', 'V.	2.19.00.01	B46-2P01-I	5_030620	17.Vgcc1Ma	inCpu-7115	784-13923	6362', 'sbin)	lubancti", '	'certi
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2029-12-3	TRUE {	"country(['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01846-2P01	1-6_03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6_0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz <sup>1</sup> , 'V.	2.19.00.01	B46-2P01-I	5_030620	17.Vgcc1Ma	nCpu-7115	784-13923	6362', 'sbin)	lubancti", '	'certi
RSA	4096 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2038-07-3	TRUE {	"country(['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01846-2P01	1-6_03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6_0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz <sup>1</sup> , 'V.	2.19.00.01	B46-2P01-I	5_030620	17.Vgcc1Ma	inCpu-7115	784-13923	6362', 'sbin)	lubancti", '	'certi
ECDSA	384 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2038-01-1	TRUE {	"country" ['s	ample C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01846-2P01	1-6 03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6 0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz <sup>1</sup> , 'V.	2.19.00.01	B46-2P01-I	5 030620	17.Vgcc1Ma	inCpu-7115	784-13923	6362', 'sbin	lubancti", '	'certi
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2029-12-3	TRUE {	"country" ['s	ample C2.z	ip', 'VSWc2/N	VMe/ssd	/1/version/V	ER/V2.19.00.	01846-2P01	1-6 03062017	7.Vgcc1Ma	inCpu', 'V2.1	9.00.01846-	2P01-6 0306	2017.Vgc	c1MainCp	u-7115784	-1392363	62.gz <sup>1</sup> , 'V.	2.19.00.01	B46-2P01-I	5 030620	17.Vgcc1Ma	inCpu-7115	784-13923	6362', 'sbin	lubancti", '	'certi
RSA	4096 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2042-01-1	TRUE {	"country" ['s	ample C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt_uti	lity/mml/sou	urce/env/py	ython_lib/di	st-packag	es/certifi/ca	cert.pem']															
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2025-05-1	TRUE {	"country"["s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt_uti	lity/mml/sou	urce/env/py	ython_lib/di	st-packag	es/certifi/ca	cert.pem']															
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2037-12-0	TRUE	country ['s	ample_C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt_uti	lity/mml/sou	urce/env/py	ython lib/di	st-packag	es/certifi/ca	cert.pem"															
RSA	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY	-	2029-12-3				ip', 'VSWc2/N																							
RSA	4096 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2038-07-3	TRUE {	country []'s	ample C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt uti	lity/mml/sou	urce/env/py	ython lib/di	st-packag	es/certifi/ca	cert.pem"															
ECDSA	384 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2038-01-1	TRUE	country i's	ample C2.z	ip', 'VSWc2/N	VMe/ssd	/weblmt uti	lity/mml/sou	urce/env/pv	ython lib/di	st-packae	es/certifi/ca	cert.pem'l															
RSA	1024 PEM			BEGIN PUBLIC KEY						ip', 'VSWc2/N									1														
								-,			,			1																			
$\langle \rangle$	C2 infoleak-a	cummatric	mublic																			_			_		_						
		-,	- Panne																														ſ

Figure 53: C2 Symmetric keys (Black Duck)

	A	8	
Email		file	Domain
posix-renam	ne@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0beb1dd214020cd9bb48fcd9225ab670fff93884d74e3d8198e4eafec1aab089/diff/lib/libsftp.so']	openssh.com
iangjiwei3@	@zte.com.cn	['sample_C2.zip', 'VSWc2/NVMe/docker/image/overlay2/imagedb/content/sha256/050e2f258d5573f1f000b10fb47458f0e95f3a0d6ee50a4825b5bdf5f2c26d34']	com.cn
nmac-md5-9	96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh']	openssh.com
lib@opens	sh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh']	openssh.com
eow@open	issh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh']	openssh.com
nmac-md5-9	96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
lib@opens	ssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
mac-md5-9	96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
lib@opens	sh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
mac-md5-9	96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh']	openssh.com
lib@opens:	sh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh']	openssh.com
ow@opens	ssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh']	openssh.com
mac-md5-9	96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
lib@opens	sh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
mac-md5-9	96-etm@openssh.com	[sample_C2.zip], VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb2zc700acaf617f210a1e3e25c5dfd478ec/diff/client.tar, 'usr/libexec/openssh/ssh-keysign']	openssh.com
lib@opens	sh.com	[sample_C2.zip], VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb2zc700acaf617f210a1e3e25c5dfd478ec/diff/client.tar, 'usr/libexec/openssh/ssh-keysign']	openssh.com
fo@pytho	onware.com	[sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/re.py]	pythonware.co
evans@cle	ear.net.nz	[sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb718436322f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/smtplib.py]	net.nz
_	onware.com	[sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/xmlrpclib.py]	pythonware.c
Irake@acm		[sample C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/distutis/sysconfig.py"]	acm.org
	D0888@cougar.noc.ucla.edu	[sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email.py]	ucla.edu
ngel1@co	ugar.noc.ucla.edu	[sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email.py]	ucla.edu
		[sample C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/li	sourceforge.n
	1.110929.45684@aaa.zzz.org	[sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/lib/	zzz.org
	eecs.umich.edu	Sample C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/python2.7/lib/p	umich.edu
	D0888@cougar.noc.ucla.edu	(sample C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.712/lib/python2.712/	ucla.edu
	ugar.noc.ucla.edu	[sample C2.zip], VSWc2/NVMe/docker/overlav2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.712/lib/python2.712/	
-	•	[sample C2.zip], VSWc2/NVWe/docker/overay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e374887c57/diff/home/weblmt/env/python2.712/lib/python2.7/email/test/test email renamed.py	
	1.110929.45684@aaa.zzz.org	[sample C2.zip], VSWc2/NVMe/docker/overlav2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.712/lib/python2.712/	
	eecs.umich.edu	[sample C2.zip], VSWc2/NVMe/docker/overlav2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.712/lii//yython2.712/lii//yython2.712/lii/	
-	1.110929.45684@aaa.zzz.org	1 minute_categy / www.clww.classes.com/www.classe	zzz.org
	1.110929.45684@aaa.zzz.org	1 ample	zzz.org
	713530.98441@python.org	Lampe_cutpy / SWc2/WWe/docker/overlag/21412d8ba8/b718436322f8512f64721512358/d161317e1e2e37448975/7/diff/home/weblmt/en/python2.712/lib/python2.7/email/est/data/msg 06.1t1	python.org
	1.110929.45684@aaa.zzz.org	1 ample_cutpy / SWc2/WWe/docker/overlag/21412d8b8db718436322f8512f6472151235b4161317e1e2e374489757/diff/home/weblmt/en/python2.712/lii/python2.7/email/est/data/msg 14.1t1	zzz.org
	D0888@cougar.noc.ucla.edu	[ zmipe	ucla.edu
	ugar.noc.ucla.edu	Lample_cutpy_towney/output/output/21412dbbbdf/18436322fb51726472151235b3fd16317fe1e2e374489757/diff/home/webmit/env/prtonz.7.12/lii/pottonz.7/email/est/data/msg_toxty_t	ucla.edu
· -	@socal-raves.org	[sample_c_lp], vsw2/vvwe/jocker/vverag/2/14/Lab8badf/15/149632226517/c0/21/Lab3badf/25/16/227657/diff/home/we/badf/20/10/21/Lab3badf/25/2001/25/16/2001/25/2001/25/16/2001/25/2000	socal-raves.or
	DOB8X@cougar.noc.ucla.edu	Lamipe C.L.D., Vawc2/WWW/Budder/Verlag/21412088bd/T3483227851724/2112132363dfb31784/211782630103917842257451744876374fb784876374fb78487647947b174.7121/bj0ython7.2122/bj0ython7.2122/bj0ython7.2122/bj0ython7.2122/bj0ython7.2122/bj0ython7.2122/bj0ython7.	ucla.edu
	4.110929.45684@aaa.zzz.org	Lamipe_c.c.di, vawc/www.euodee/wenia/21412088bdf/13483227851726472112323361618717e1ze23740477612e1ze374487637416/mee/welmit/emity/product.r.1210/bj/python2.r210012/jeminy/guagimag_toxti	zzz.org
	www.linux.org.uk	[smip:_c.c.n], vswc/www.euocer.vering/21412088bdf/1348322285172647211232336161871e2ie237437672612701701110012794400117.121010017.1210017.1210017.121010017.121010017.12100	org.uk
-			
050.01304	4.110929.45684@aaa.zzz.org C2 infoleak-emails	['sample_C2.zip', VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_29.txt']	zzz.org

Figure 54: C2 Infoleak email addresses (Black Duck)

A	В	C	D	E	F	G	н	1.1	J	K	L
1 IP	IPv6	File									
2 0.0.0.0	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
3 127.0.0.0	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
4 8.8.8.8	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
5 8.8.4.4	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
5 2001:4860:4860::	8844 TRUE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
7 2001:4860:4860::	8888 TRUE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
9 192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
0 173.1.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
1 173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
2 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
3 192.254.1.18	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
4 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1a674e05a	1905d949c	bd6e1ef8	7343e9b89	ada46dbef4	1afd69ea	987c16d71	/config.v2.j	son']
5 192.254.128.1	FALSE	['sample C2.zip', 'VSWc2/NVMe/docker/containers/0	1a674e05a	1905d949c	bd6e1ef8	7343e9b89	ada46dbef4	1afd69ea	987c16d71	/config.v2.j	son']
6 173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1a674e05a	1905d949c	bd6e1ef8	7343e9b89	ada46dbef4	1afd69ea	987c16d71	/config.v2.j	son']
7 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1a674e05a	1905d949c	bd6e1ef8	7343e9b89	ada46dbef4	1afd69ea	987c16d71	/config.v2.j	son']
8 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1e6cd8f54c	99067f2bb	3a011f3bb	05ad9d79d	lb98c377024	4fe81862c	351da7b/	config.v2.js	ion']
9 192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1e6cd8f54c	99067f2bb	3a011f3bb	05ad9d79d	lb98c377024	4fe81862c	3351da7b/	config.v2.js	ion']
0 173.1.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1e6cd8f54c	99067f2bb	3a011f3bb	05ad9d79d	b98c377024	4fe81862c	351da7b/	config.v2.js	ion']
1 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1e6cd8f54c	99067f2bb	3a011f3bb	05ad9d79d	b98c377024	4fe81862c	351da7b/	config.v2.js	ion']
2 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1f66129374	2bb28efab	029b6d4a2	20bef338d	lf4e70c5e5	dc08302f40	)60e0558/0	config.v2.js	on']
3 192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1f66129374	2bb28efab	029b6d4a2	20bef338d	lf4e70c5e5	dc08302f4	)60e0558/0	config.v2.js	on']
4 173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1f66129374	2bb28efab	029b6d4a2	20bef338d	lf4e70c5e5	dc08302f4(	)60e0558/0	config.v2.js	on']
5 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	1f66129374	2bb28efab(	029b6d4a2	20bef338d	lf4e70c5e5	dc08302f40	60e0558/0	config.v2.js	on']
6 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	2fde1b64f4	990366ac3e	b11ac0e7	f50e1b448	46acaec81a	7a9f250b6	6bf0e47/c	onfig.v2.js	on']
7 192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	2fde1b64f4	990366ac3e	b11ac0e7	f50e1b448	46acaec81a	7a9f250b6	6bf0e47/c	onfig.v2.js	on']
8 173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									
9 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	2fde1b64f4	990366ac3e	b11ac0e7	f50e1b448	46acaec81a	7a9f250b6	6bf0e47/c	onfig.v2.js	on']
0 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	7824cdfd82	9065f53ad1	bd8acb36	33c2dfb5a	c3f6887a03	252c3cebd	a9b4d57/c	onfig.v2.js	on']
1 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	7824cdfd82	9065f53ad1	bd8acb36	33c2dfb5a	c3f6887a03	252c3cebd	a9b4d57/c	onfig.v2.js	on']
2 127.0.0.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	7824cdfd82	9065f53ad1	bd8acb36	33c2dfb5a	c3f6887a03	252c3cebd	a9b4d57/h	nosts']	
3 8.8.8.8	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	7824cdfd82	9065f53ad1	bd8acb36	33c2dfb5a	c3f6887a03	252c3cebd	a9b4d57/r	esolv.conf	]
4 8.8.4.4	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	7824cdfd82	9065f53ad1	bd8acb36	33c2dfb5a	c3f6887a03	252c3cebd	a9b4d57/r	esolv.conf	1
5 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									
6 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									
7 127.0.0.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0	880e826c20	)5d9417dc8	954bcb785	f3799e049	719441ac52	631a8081	9a7020e/ł	hosts']	
8 8.8.8.8	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									1
9 8.8.4.4	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									-
0 192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									-
1 173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0									
2 127.0.0.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0								· ·	
	C2 infoleak-ips	+								•	



1	ь.	5

Address	Vendor	File
00:00:00:FF:FF:FF	Officially Xerox	Tsamole (2,zid), VSWc2/WVWe/docker/overlapi2/46)8a6a791fthc31a6a6498447le524495dbc6cf7ac72db8a24295ce289f5ee/diff/tmo/ MEInSomib/libovthon2,7,so.101
00:60:08:11:CE:4E	3Com 3Com PCI form factor 3C905 TX board	["sample_C2.zig/, VSWc2/WVWe/docker/overlap2/dd7c56de82dz36497dd229b5xd4be120b8/dddbb413d304995576308d1d4e74/diff/etc/udhcpd.conf"
00:60:08:11:CE:3E	3Com 3Com PCI form factor 3C905 TX board	['sample (2.1:p', 'NSW2]/WMe[docker/over/ay2/4d7h56de82ds256574d2s95576308d1d4e74/diff/etc/udhtpd.conf]
00:00:00:FF:FF:FF	Officially Xerox	[sample C2.1p], VSW2/WVMe/docker/over/ay2/Se126531b416431fcs51d2828f0637bbfd1888fe206877a4bdbt024266ee9a/diff/home/webmnt/backend/webmnt/, llboython2.7.so.1.0]
00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', VSW2/IVVMe/docker/over/ar2/8963He01575H6fe601164a596596eB1.c51aa8H89ee72/e1297043b64a9a13d/dfff/etc/network/interfaces]
00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C2.zig/, VSWc2/WVWe/docker/overtay2/8e5612675xc2/d19beba7259999f5x51edba136a70d3x2287890d90de08980c/dff/vm_deplov,ison1
00:11:22:33:44:55	CIMSYS Inc	['sample_C2.1g', VSW2]/VVMe[docker/over/ay2/c71/059508d9884e6/c766/560b663e9/t11681b162db2/d17ee8d:649aaaba/d/t1f/etc.nommu/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	[sample C2.1g/, VSW2]/VVMe[docker/over/ay2/C1109980849884e6it7661566b663e9ft11681b162/bc17e686:649aaaba/diff/etc/network/Interfaces]
00:11:22:33:44:55	CIMSYS Inc	[sample (2.1;c), VSW2]/VVMe[docker/overlag2/c90971d80455ee1bbe8400:de7821cr12e3dbb58aeff5695131cr281254d3)ddff/ors-busybox@846-2901-6.tar/, %7641745df2b12c74435febc46e3baefeae8b5412b4297d96631111ab68092/layer.tar/, *tc.nommu/network/interfaces7
00:11:22:33:44:55	CIMSYS Inc	['sample_C2.ip], VSWc2/WVMe/docker/over/ar2/c509571d80455ee1bbe84a0:5e7821cr12e3dbb58aef5069:131cce312b4d3/ddff/ors-busybox@846-2001-6.tar/, '87b41745df2b112;714385feb:G46e3baeReae8b5412b4297d9d631111ab68092/layer.tar', 'etr/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	[sample (2.1);/ VSW2]/VV/e[docker/over/ay2/fe0ds221e31051aa5ed4a637hbbaf5210872ab.20b4d304f5584564a846504621e53/diff/oss-busybougB46-2901-6.tar/, %7b41745df2b1274835febc546e3bae0eae8b5412b4257d56631111ab68892/layer.tar/, *etc.nommu/network/interfaces?]
00:11:22:33:44:55	CIMSYS Inc	[sample (2.1)], VSW2]/VV/e[docker/over/ay2]/fe0d8221e31051aa4ed4a637bbba45210872ab28b463444559490a48dódz2e52/diff/oss-basybougB46_3901-6.tar', %7b41745df2b1274885febc46e3bae0eae8b5412b4297896631111ab68092]/ayer.tar', *tc/network/interfaces7
00:A0:C9:00:00:02	Intel	['sample (2.zip', VSW2)/VMe/logs/litepaas/jomslave.log']
00:00:00:00:01:00	Officially Xerox	['sample_C2.tip', VSWc2/WVMe/logs/litepaas/jpmslave.log']
00:01:02:03:04:05	BBN	['sample C2.zip', VSWc2/WVMe/ssd/1/version/VER/V2.15.00.01846-2P01-6 03062017.Vbpc5Cpu-/2005181-13351964,gz', \u00f5fu-img', \
00:11:22:33:44:55	CIMSYS Inc	[sample C2.1p], VSWs2/WVMe[ssd/1/version/VER/V2.19.00.01846-2901-6 03662017.Vbpc5Cpu/, V2.19.00.01846-2901-6 03662017.Vbpc5Cpu-2805181-13351964.gz/, luboot-fw.img', luboot-fw.img', VAT-DET
00:12:34:56:78:90	Camille Bauer	[sample C2.zip], VSWs2/WVMe[ss0/1/version/VER/v2.19.00.01846-2P01-6 03662017.Vbpc5Cpu/, V2.19.00.01846-2P01-6 03662017.Vbpc5Cpu-2805181-13351964.gz/, \u00ffwimg,
00:11:22:33:44:55	CIMSYS Inc	[sample (2.1)]/ VSW2/WWe/ssd/1/version/VER/V219.00.01846-2901-6 08602017/Vbpc5Cpv/, V219.00.01846-2901-6 03602017/Vbpc5Cpv-2805181-13351944.gt/, \u00ffwimg', \u0
00:a0:c9:00:00:02	Intel	['sample (2.1)/, 'NSW2]/V/Me/ssd/1/version/VER/V2.19.00.01046-2901-6 08062017.Vgcc1MainCpu-711578-139286862.gz', 'V2.19.00.01046-2901-6 08062017.Vgcc1MainCpu-711578-139286862,gz', 'V2.19.00000000000000000000000000000000000
00:a0:c9:00:00:00	Intel	[sample C2.1g/, VSWz]/VVMe[ssd/1/version]VER/V2.19.00.01846-2901-6 03662017.Vgcc1MainCpu/, V2.19.00.01846-2901-6 03662017.Vgcc1MainCpu-7115784-13928662, gz/, V2.19.00000000000000000000000000000000000
00:11:22:33:44:55	CIMSYS Inc	['sample (2.1;0', VSWz]/VVMe/ssd/1/version/VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139236362,gr', V2.19.00.01846-2901-6 03062007.Vgcc1MainCpu-7115784-139236362,gr', V2.19.00.01846-2901-6 03062007.Vgcc1MainCpu-7115784-139236362, boot/hdump.cpin.egr', etc/network/interfaces/]
00:11:22:33:44:55	CIMSYS Inc	[sample (2.2)p/, VSWc2/NVMe/ss/1/uersion/VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139236632.gr, V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-13923632.gr, V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-13923632.gr, V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-13923632.gr, V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-13923632.gr, V2.19.00.01846-2901-6 03062017.gr, V2.19.00000000000000000000000000000000000
00:11:22:33:44:55	CIMSYS Inc	['sample (2.1)/, 'NSW2/NVMe/ssd/1/version/VER/V2.19.00.01846-2901-6 03662017.Vgcc1MainCpu-7115784-135286362, gz', V2.19.00.01846-2901-6 03662017.Vgcc1MainCpu-7115784-135286362, gz', gz', gz', gz', gz', gz', gz', gz'
00:a0:c9:00:00:02	Intel	[sample C2.1g/, VSWs2]/VMe[ssd]/Iversion]VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, gz', V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, gz', V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, for each of the second s
00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	[sample C2.zip], VSWs2/WVMe/ss3/1/version/VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139236362,gr, V2.19.00.01846-2901-6 03062007.Vgcc1MainCpu-7115784-139236362,gr, V2.19.00.01846-2901-6 03062007.Vgcc1MainCpu-7115784-139236362, predoct/mamilsk.bin/, 'boot.out']
00:11:22:00:11:22	CIMSYS Inc	[sample C2.zig/, VSWc2/WVWe/ssd/1/version/VER/V219.00.01846-2P01-6 03062017.Vecc1MainCpu/-7115784-13923662.gz/ V2.19.00.01846-2P01-6 03062017.Vecc1MainCpu/-7115784-13923662.gz/
00:11:22:00:44:55	CIMSYS Inc	[sample_(22.1p], VSWc2/NVMe/ss/1]/version/VER/V2.19.00.01846-2901-6_03662017.Vgcc1MainCpu <sup>-</sup> 7115784-13923663Lgr, V2.19.00.01846-2901-6_03662017.Vgcc1MainCpu <sup>-</sup> 7115784-13923682Lgr, V2.19.00.01846-2901-6_0362017.Vgcc1MainCpu <sup>-</sup> 7115784-13923682Lgr, V2.19.00.01846-2901-6_03662017.Vgcc1MainCpu <sup>-</sup> 7115784-13923682Lgr, V2.19.00.01846-2901-6_03662017.Vgcc1MainCpu <sup>-</sup> 7115784-13923682Lgr, V2.19.00.01846-2901-6_03662017.Vgcc1MainCpu <sup>-</sup> 7115784-13923682Lgr, V2.19.000000-0000-0000-0000-0000-000-000-000
00:a0:c9:00:00:00	Intel	[sample C2.1g/, VSWs2]/VMe[ssd]/Iversion]VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, gz', V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, gz', V2.19.0002, gz', W2.19.0002, gz
00:11:22:00:00:22	CIMSYS Inc	[sample (2.zip/, VSWc2/WWe/ss/]/version/VEI/V219.00.01845.2901-6 03062017.vgcc1MainCpu/, Y219.00.01845.2901-6 03062017.vgcc1MainCpu/, 7115784-13923630.zgr, Y2.19.00.01845.2901-6 03062017.vgcc1MainCpu/, 7115784-13923630.zgr, Y2.19.00.01845.2901-6 03062017.vgcc1MainCpu/, Y219.00.01845.2901-6 03062017.vgcc1MainCpu/, Y219.000000000000000000000000000000000000
00:11:22:33:44:55	CIMSYS Inc	[sample (2.1)], VSW2]/VMe/ssd/1/version/VER/V219.00.01046-2901-6 03062017.Vgcc1MainCpu-7115784-139236362,zr, V2.19.00.01046-2901-6 03062017.Vgcc1MainCpu-7115784-139236362, zr, V2.19.00.01047
00:11:22:33:44:55	CIMSYS Inc	[sample C2.10], VSW2/WVMe/ssd/1/version/VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-135236362, gz, V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-135236362, gz, V2.19.00000000000000000000000000000000000
00:11:22:33:44:55	CIMSYS Inc	[sample C2.1g/, VSWz]/VMe[ssd/1/version]VER/V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, gz', V2.19.00.01846-2901-6 03062017.Vgcc1MainCpu-7115784-139286362, gz', V2.19.0002, gz', V2.19.0002, gz', W2.19.0002, gz'
00:00:00:FF:FF:FF	Officially Xerox	[sample (2.2)p/, VSWc2/WVMe/ss/j/uersion/VEV/219.00.01845-2901-6 03062017.vgcc1MainCpu-7115784-13923680.zgr, V2.19.00.01845-2901-6 03062017.vgcc1MainCpu-7115784-1392680.zgr, V2.19.00.01845-2901-6 03062017.vgcc1MainCpu-7115784-1392680.zgr, V2.19.00.01845-2901-6 0306200-000000000-0000-0000-0000-0000-00
00:00:00:FF:FF:FF	Officially Xerox	[sample (2.1)], /SWk2]/V/Me/ssd/1/version/VER/V219.00.01046-2901-6 03062017.Vgcc1MainCpu-/115784-135236362,zr, /V219.00.01046-2901-6 03062017.Vgcc1MainCpu-/115784-135236362,zr, /V219.00.01046-2901-6 03062017.Vgcc1MainCpu-/115784-135236362, bin/lubanslave/, liboyrthon2.7.so.1.0]
00:11:22:33:44:55	CIMSYS Inc	['sample C2.1g/, VSWz]/V/We/ssd/1/version/VER/V2.19.00.01846-2 02191718.Pb1124fCpu/, V2.19.00.01846-2 02191718.Pb1124fCpu-3445832-7314621_gz/ vboot-fw.img/ vbcot-fw.img/
00:00:00:00:01:00	Officially Xerox	[Sample C2.2ip', VSWc2]/WMe/ss/J859/dmesg.log1
00:a0:c9:00:00:02	Intel	[sample (2.sip/ VSWs2)/VMe/ssd/859/dmess.log"
00:a0:c9:00:00:00	Intel	Tsample C2.sid/, VSWc2/NVMe/ssd/859/dmess.log1
00:00:00:00:01:00	Officially Xerox	Tsample C2.tid/, VSWc2/NVMe/sd/859/dmeg.old.log1
00:a0:c9:00:00:02	Intel	Sample C2.zip/, VSW2/VVMe/ssg/859/dmesg old.log
00:00:09:00:00:00	Intel	Tsmple C2.air/, VSWc2/WWe/sd/889/dmesc old.bg1

### Figure 56: C2 Infoleak MAC addresses (Black Duck)

A	В	С	D	E	F	G	H		1	J	K	L	M	N	0		P	Q	R	S	T	U	V	W	Х	Y	Z	AA	AB	AC	AD	AE	AF
Password	User	Algorithm	Salted	Hashed	File																												
L87R/0xbslriY	ftpuser	DES	FALSE	TRUE	['sample_	C2.zip',	VSWc2/I	/VMe/do	cker/ov	erlay2/1b9	88acedd	72a966be	2400ce9a	b0177123	bd5d2e5e2	45063eff	f78a492	761499	/diff/etc/p	passwd']													
gs801.dk5eWHE	root	DES	FALSE	TRUE	['sample_	C2.zip',	VSWc2/I	/VMe/do	cker/ov	erlay2/1b9	88acedd	72a966be	2400ce9a	b0177123	bd5d2e5e2	45063eff	f78a492	761499	/diff/etc/p	passwd']													
gs801.dk5eWHE	root	DES	FALSE	TRUE	['sample_	C2.zip',	VSWc2/I	/VMe/do	cker/ov	erlay2/1b9	8acedd	72a966be	2400ce9a	b0177123	bd5d2e5e2	45063eff	f78a492	761499	/diff/etc/p	passwd-']													
TWSiviK7uPtsw	ftpuser	DES	FALSE	TRUE	['sample_	C2.zip',	VSWc2/I	wMe/do	cker/ov	erlay2/214	12d8b8	dfb71843	63222f85	172f64721	51235b3fd:	16317fe1e	e2e3744	197c57/0	diff/etc/pa	asswd"]													
vY17tW3kiRlADnks0lgyJ0	root	MD5	TRUE	TRUE	['sample_	C2.zip',	VSWc2/I	wMe/do	cker/ow	erlay2/214	12d8b8	dfb71843	63222f85	172f64721	51235b3fd	16317fe1e	e2e3744	197c57/0	diff/etc/pa	asswd"]													
	root		FALSE	FALSE	['sample	C2.zip',	VSWc2/I	evMe/do	cker/ow	erlay2/4df	7c56de8	82da2649	74d2a9b5	c84bef20b	8fdddbb4	f3d30499	95763080	1d4e74	/diff/etc/s	shadow']													
CDPT6wiRvyCmIGktNgQ1/	root	MD5	TRUE	TRUE	['sample_	CZ.zip',	VSWc2/I	evMe/do	cker/ow	erlav2/896	3fe01f5	75f6fe60	1164a5b8	596e61c35	1aaSf89ee	72fe1797	043b64a	9a13d/d	liff/etc/pa	isswd"]													
W17tW3kiRlADnks0lgvJ0	root	MD5	TRUE		['sample																												
Y17tW3kiRIADnks0lgvJ0	root	MD5	TRUE	TRUE																	B45-2P01-	6.tar', '87b	1745df2b1	2c724385	febc945e3b	ae0eae8b	5412b4297	d9d631111a	b68092/lav	er.tar'. 'et	c/passwd"		
Y17tW3kiRlADnks0lgvJ0	root	MD5	TRUE	TRUE	['sample																												
vY17tW3kiRlADnks0lgvJ0	root	MD5	TRUE																		B46-2P01	-6.tar', '87b	41745df2b	12:724389	ifebr946e3	haeOeae8	54125429	d9d631111	b68092/la	ver.tar'. 'e	tc/passwd1		
vY17tW3kiRlADnks0lgvJ0	root	MD5	TRUE		['sample																												
vY17tW3kiRlADnks0lgyJ0	root	MDS	TRUE																									ainCpu-711	784,13923	6367 'hor	t/kdump o	nio ez' 'et	e/naccu
HzcOyOx1na4oQJDFZcOR7/	admin	MDS	TRUE																									ainCpu-711					
nrRxdGlHdg0ckqS9kS85A1	zte	MDS	TRUE																									ainCpu-711					
rSltymrJ8GbXV36YcjCZ.	root	MD5	TRUE																									ainCpu-711				ck hin' 'a	trichar
rSitymrJ8GbXV36YcjCZ.	zte	MD5	TRUE																									ainCpu-711					
Y17tW3kiRlADnks0lgyJ0	root	MD5	TRUE		['sample																							unicpu / 12	104 10010	iosor, pro	boot frame	onen, c	ccy and
1171W3KIKIRDINSUISYD	TOOL	MIDS	INCE	TRUE	[ sample_	ceap,	vonczy	www.ej sou	al ti vers	UN VERY	2.13.00	01040-2	0215171		.pu, v2.1		0-2_0215	1/10.91	1124/cpu-	-3443032-1	1214021-8	2, 00000-11	v.iiiig, uu	obe-tw.iii	g, eurpas	swuj							
C2 infoleak-page	swords	+																					_	_	_	_	_	_	_	_	_	_	-

\_\_\_\_

Figure 57: C2 Infoleak password (Black Duck)

Url	File	Domain
http://zlib.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlav2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	zlib.net
http://apr.apache.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	apache.org
http://www.libexpat.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlav2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	libexpat.org
http://httpd.apache.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	apache.org
http://alpinelinux.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	alpinelinux.org
http://www.gnu.org/software/gzip	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	gnu.org
http://busybox.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	busybox.net
http://www.gnu.org/software/ncurses	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	gnu.org
http://packages.debian.org/sid/ca-certificates	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	debian.org
http://www.musl-libc.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	musl-libc.org
http://openssl.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	openssl.org
http://git.alpinelinux.org/cgit/apk-tools	['sample_C2.zip', 'VSWc2/NVMe/docker/overlav2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	alpinelinux.org
https://wiki.gentoo.org/wiki/Hardened/PaX Utilities	['sample_C2.zip', 'VSWc2/NVMe/docker/overlav2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	gentoo.org
http://lynx.invisible-island.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	invisible-island.ne
http://git.kernel.org/cgit/utils/util-linux/util-linux.git	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	kernel.org
http://git.alpinelinux.org/cgit/aports/tree/main/alpine-baselayout	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	alpinelinux.org
http://zlib.net	['sample_c2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	
http://alpinelinux.org	['sample_C2.zip', VSWc2/NVMe/docker/overlay2/ddf7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	
http://busybox.net	['sample_c2.zip', 'VSWc2/NVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	
ttp://www.musl-libc.org	[sample_c2:rip], VVVc2/VVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed"]	
ttp://openssl.org	[sample_czzip], VVVc2/VVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed"]	•
ttp://git.alpinelinux.org/cgit/apk-tools	[sample_cz.zip], vswc2/NVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed"]	
http://wiki.gentoo.org/wiki/Hardened/PaX_Utilities	[sample_cz.zip], vswc2/NVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed"]	
	[sample_cz.zip], vswc2/NVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed"] ['sample_c2.zip', 'vsWc2/NVMe/docker/overlay2/4d7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed"]	• •
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/rct-agent/pods/0	[sample_cz.zip], vswcz/wwwe/uocker/overia/z/40/vsoueozuazo49/40/zasusca40erzouoroduo0450504555576506010442/4/um/m0/apk/do/mstaned ] ['sample_cz.zip', VsWc2/NVMe/dockerd.log']	Unknown
http://173.254.95.16:9099/lpm/fileServer/modelData/v2.00.21.01P01R07		Unknown
ittp://192.254.1.16:8098/api/v1/namespaces/1/rcs/ce1m/pods/0	['sample_c2.zip', VSWc2/NVMe/dockerd.log']	Unknown
	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/lccm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/dpf-dts/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/udc/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
C2 infoleak-urls +		

### Figure 58: C2 Infoleak URLs (Black Duck)

A	В	C	D	E	F		н	1	1		ĸ		- h-	M		N	0	<i>v</i>
Component		Latest ve		Matching type	CVSS		Object compilation date			I Object SHA1				CVSS vector (v2)	CVSS vector		Summary	Distribution pack
Flask		2.2.2	CVE-2019-1010083	Exact match			2019-03-06T12:35:22Z					9888f60c57d64b6		.5 AV:N/AC:L/Au:N:/C:N/I:N/A:P		R:N/UI:N/S:U/C:N/I:N/A:H		
Flask		2.2.2	CVE-2019-1010083	Exact match		5 2019-07-17714:15:002	2019-03-06712:35:222					05e95c4e890f197		5 AV:N/AC:L/Au:N:/C:N/I:N/A:P		R:N/UI:N/S:U/C:N/I:N/A:H		
Flask		2.2.2	CVE-2023-30861	Exact match		3.7 2023-05-04708:43:232	2019-03-06T12:35:22Z	METADAT	sample_	C 1ab20209f45f3d	17a6b186af51	9888f60c57d64b6		5	AV:N/AC:L/P	R:N/UEN/S:U/C:H/EN/A:N/E:U/RE:O/RC:C		
Flask	0.12.2	2.2.2	CVE-2023-30861	Exact match		3.7 2023-05-04T08:43:232	2019-03-06T12:35:22Z	niem	sample	C cc25140d669bc8	69681524240	66e95c4e890f197	6	5	AV:N/AC:L/P	R:N/UEN/S:U/C:H/EN/A:N/E/U/RL:O/RC:C		
Flask	0.12.2	2.2.2	CVE-2018-1000656	Exact match		3.7 2019-03-25717:16:192	2019-03-06712:35:222	METADAT	sample_	C 1ab20209f45f3d	j7a6b186af51	9888f60c57d64b6	4	.6	AV:N/AC:L/P	R:N/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:C		
Flask	0.12.2	2.2.2	CVE-2018-1000656	Exact match		3.7 2019-03-25717:16:192	2019-03-06T12:35:22Z	main	sample	C cc25140d669bc6	696815a4a4er	66e95c4e890f197	4	6	AV:N/AC:L/P	R:N/UEN/S:U/C:N/EN/A:L/E:U/RL:O/RC:C		
apk-tools	2.6.9-10		CVE-2021-30139	Exact match		5 2021-04-21716:15:002	2017-06-23107:13:202	apk	sample	C 6b7cc7b1871071	1671949c8a41	c39ed4de091b17	7	5 AV:N/AC:L/Au:N:/C:N/I:N/A:P	AV:N/AC:L/P	R:N/UI:N/S:U/C:N/I:N/A:H		alpine
apr	1.5.2-r0	1.7.4	CVE-2022-28331	Exact match		5.5 2023-02-01710:09:112	2016-04-29T16:50:46Z	libapr-1.si	sample	C 26830da1019db	94c12057268	16a4aa1492942f;	. 8	5	AV:N/AC:L/P	R:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C		alpine
apr	1.5.2-10	1.7.4	CVE-2022-24963	Exact match		5.5 2023-02-01710:06:382	2016-04-29716:50:462	libapr-1.5	sample	C 26830da1019db	94c12057268	516a4aa1492942f;	8	5	AV:N/AC:L/P	R:N/UEN/S:U/C:H/EH/A:H/E/U/REO/RC:C		alpine
apr	1.5.2-0	1.7.4	CVE-2017-12613	Exact match		1.6 2018-01-08T16:19:392	2016-04-29716:50:462	libapr-1.se	sample	C 26830da1019db	94c12057268	516a4aa1492942f;	5	4	AV:L/AC:L/PE	R:N/UEN/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C		alpine
apr-util	15.4-11	1.6.3	CVE-2022-25147	Exact match		3.7 2023-02-14714:59:412	2016-08-12709:38:102	libaprutil-	sample	C 78983ae3fdfc64	8010287261a	2128451c801f61d	- 6	5	AV:N/AC:L/P	R:N/UEN/S:U/C:N/EN/A:H/EU/REO/RC:C		aloine
apr-util	154-11	1.6.3	CVE-2017-12618	Exect match		1.6 2018-01-0ET16:38:082	2016-08-12709:38:102	libaorutil-	sample	C 78983ae3fdfc64	8010287261	2128451c801f61d	5	4	AV:L/AC:L/PI	R:N/UEN/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C		alping
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match		10 2014-09-28T19:55:007	2018-07-24701:54:272			C 2bc290ff789dc0				0 AV:N/AC:L/Au:N:/C:C/I:C/A:C				
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match		10 2014-09-28719:55:002	2018-07-24101-54:272			C 2bc290ff789dc0				0 AV:N/AC:L/Au:N:/C:C/I:C/A:C				
bash		5.2.15	CVE-2014-7169	Exact match		10 2014-09-25701:55:002				C 2bc290ff789dc0				0 AV:N/AC:L/Au:N:/C:C/I:C/A:C				
bash		5.2.15	CVE-2014-6278	Exact match			2018-07-24T01:54:272			C 2bc290ff789dc0				0 AV:N/AC:L/Au:N:/C:C/I:C/A:C				
bash		5.2.15	CVE-2014-6277	Exact match			2018-07-24T01-54:272			C 2bc290ff789dc0				0 AV:N/AC:L/Au:N:/C:C/I:C/A:C				
bash		5.2.15	CVE-2016-7543	Exact match			2018-07-24101:54:272			C 2bc290ff789dc0				5	ANH (ACH JR	R:L/UEN/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C		
bash		5.2.15	CVE-2019-18276	Exact match			2018-07-24T01:54:27Z			C 2bc290ff789dc0				8		R:N/JIEN/S:U/C:H/EH/A:H/E#/REO/RC:C		
bash		5.2.15	CVE-2016-0634	Exact match			2018-07-24101-54:272			C 2bc290ff789dc0				2		PR:1/UI:N/S:C/C1/I:L/A:L/E:U/RL:O/RC:C		
bash		5.2.15	CVE-2019-9924	Exact match			2018-07-24101:54:272			C 2bc290ff789dc0			7			R:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C		
bash		5.2.15	CVE-2019-3324 CVE-2022-3715	Exact match		3 2023-01-06T12:22:07Z				C 2bc2901789dc0			5			R:L/UER/S:U/CEI/EL/A:H/E-P/RE/W/RC/C		
bash		5.2.15	CVE-2012-3715 CVE-2016-9401	Exact match			2018-07-24101:54:272			C 2bc290ff789dc0				5 AV:L/AC:L/Au:N:/C:N/I:N/A.P		R:L/UEN/S:U/C:N/I:N/A:H		
berkeleydb	5.3.28-11	3.2.13	CVE-2016-3418	Exact match			2019-03-06112-45:407					67a9bdf3ee8b28		S AV:UAC:M/Au:N:/C:R/I:N/A:C		RN/JUR/SU/CH/INFAR		ubuntu
berkeleydb	5.3.28-11		CVE-2016-0694	Exact match			2019-03-06112:45:402							8 AV:UAC:M/AUN:/CC/IC/AIC		RIN/UER/SU/CH/EH/AH		ubuntu
berkeleydb	5.3.28-11		CVE-2016-0694 CVE-2016-0692	Exact match Exact match			2019-03-06112:45:402					167a9bdf3ee8b28		8 AV:UACM/AUN//CIC/IC/AIC 8 AV:UACM/AUN//CIC/IC/AIC		RIN/UER/SEU/CH/EH/ACH		ubuntu
			CVE-2016-0692 CVE-2016-0689	Exact match			2019-03-06112:45:402					67a9bdf3ee8b28						ubuntu
berkeleydb	5.3.28-11											467a9bdf3ee8b28		8 AV:L/AC:M/Au:N:/C:C/I:C/A:C		R:N/UI:R/S:U/C:H/I:H/A:H		
berkeleydb	5.3.28-11		CVE-2016-0682	Exact match			2019-03-06712:45:402					467a90df3ee8b28		8 AV:L/AC:M/Au:N:/C:C/I:C/A:C		R:N/UER/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3606	Exact match			2019-03-06712:45:402					67a9bdf3ee8b28		7 AV:L/AC:M/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3617	Exact match			2019-03-06712:45:402					467a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UER/S:U/C:H/EH/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3616	Exact match		3.7 2017-04-24719:59:002						467a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3615	Exact match			2019-03-06712:45:402					67a90df3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3614	Exact match		3.7 2017-04-24T19:59:00Z						167a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3613	Exact match			2019-03-06712:45:402					167a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3612	Exact match			2019-03-06712:45:402					67a96df3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3611	Exact match			2019-03-06T12:45:40Z					67a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P		R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3610	Exact match		3.7 2017-04-24719:59:002	2019-03-06712:45:402	libdb-5.3.	sample_	Cedfc715c728e69	91e47817da2	167a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P	AV:L/AC:H/P	R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3609	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample	C edfc715c728e65	91e47817da2	67a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P	AV:L/AC:H/P	R:N/UER/S:U/C:H/EH/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3608	Exact match		3.7 2017-04-24719:59:002	2019-03-06T12:45:40Z	libdb-5.3.	sample	c edfc715c728e65	91e47817da2	67a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P	AV:L/AC:H/P	R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3607	Exact match		3.7 2017-04-24719:59:002	2019-03-06712:45:402	libdb-5.3.	sample	C edfc713c728e65	91e47817da2	67a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P	AV:L/AC:H/P	R:N/UER/S:U/C:H/EH/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3605	Exact match		3.7 2017-04-24719:59:002	2019-03-06T12:45:40Z	libdb-5.3.	sample	C edfc715c728e65	91e47817da2	67a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P	AV:L/AC:H/P	R:N/UER/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11		CVE-2017-3604	Exact match		3.7 2017-04-24719:59:002	2019-03-06712:45:402	libdb-5.3.	sample	C edfc715c728e89	91047817da2	67a9bdf3ee8b28		7 AV:L/AC:H/Au:N:/C:P/I:P/A:P	AV:L/AC:H/P	R:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
berkeleydb	5.3.28-11ubur	tu0.1	CVE-2016-3418	Exact match		6.9 2016-04-21T11:00:00Z	2019-07-20101:02:062	libdb-5.3.	sample	C 1baf6e75368c4a	a2e30de4267	d7fdb780a58fa19;	7	8 AV:L/AC:M/Au:N:/C:C/I:C/A:C	AV:L/AC:L/PI	R:N/UER/S:U/C:H/EH/A:H		ubuntu
berkeleydb	5.3.28-11ubur	tu0.1	CVE-2016-3418	Exact match		6.9 2016-04-21T11:00:00Z	2019-01-19711-20:422					17fdb780a58fa19;	7	8 AV:L/AC:M/Au:N:/C:C/I:C/A:C	AV:L/AC:L/PI	R:N/UER/S:U/C:H/EH/A:H		ubuntu
	C2 vulnerabilities													1.4	1114446504454655			2010/02/21

Figure 59: C2 CVEs (Black Duck)

	<sup>I</sup> CODESentru	y™		
	+ NEW SCAN		N-DAY FINDINGS 0	ZERO-DAY FINDINGS
111	Dashboard		Security	Security
	Summary		79 Artifact 92 Scan Security 92 Quality	91 Artifact Security 99 Scan Quality
0	xDevOps	$\odot$	47685 Findings 20,000 15,000	9 Findings 8 6
O	NG Evaluation	$\odot$	10,000 5,000	4 2
	NG rescans	$\odot$	Managalang Houng Paul Phagmau High Classing	0 Low Medium High Critical
:	🔇 C2 rescan			
	C1 rescan		NG rescans > C2 rescan > sample_C2.zip: 5	Scan Done, Scan Depth: Shallow

# Sample C2 Code Sentry Scan Report Excerpts

Figure 60: C2 Scan Overview (Code Sentry)



# <sup>I</sup>CODESentry<sup>-</sup>

## **N-Day Findings Summary**

Name	Version	Vendor	Security Score	Number of Vulnerabilities	Path
adios	1.13.1	unspecified	100	0	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 21412d8b8dfb7184363222f85172f6 472151235b3fd16317fe1e2e374489 7c57/diff/home/weblmt/env/python_lib/ dist-packages/ipaddress.pvc
aliyungo	20220907	unspecified	100	0	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 062b2df6984742207d8e00bca1f656 89b37fc4f39427347ef81e76d0215a da47/diff/bin/registry
apache-http-server	agb_before_aaa_ changes	unspecified	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 1993c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/sbin/checkgid
apache2	upstream-2.4.27	unspecified	100	0	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19193c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/ab
apache_http_server	2.4.33	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/sbin/rotatelogs
apache_http_server	2.4.40	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/htpasswd
apache_http_server	2.4.48	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/sbin/titcacheclean
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/ab
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/ttdbm
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/ttdigest
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/httxt2dbm
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/ VSWc2/NVMe/docker/overlay2/ 19f93c843662c21857ec5e20cbc323 785e9c72dbfef9c54237b16ccf3859 4798/diff/usr/bin/logresolve

www.grammatech.com

Page 738 / 1292

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 61: C2 N-day findings (Code Sentry)



<sup>I</sup>CODESentry<sup>-</sup>

## Zero-Day Findings

Findings for sample\_C2.zip

#### Scan Depth: Shallow MD5: cc85e13f29d2a025a66c62ef25172e4a

#### Top 25 CWE Findings

Rank	ID	Name	Instances
1	CWE:787	Out-of-bounds Write	-
2	CWE:79	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	-
3	CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0
4	CWE:20	Improper Input Validation	-
5	CWE:125	Out-of-bounds Read	-
6	CWE:78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0
7	CWE:416	Use After Free	0
8	CWE:22	Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")	-
9	CWE:352	Cross-Site Request Forgery (CSRF)	-
10	CWE:434	Unrestricted Upload of File with Dangerous Type	-
11	CWE:476	NULL Pointer Dereference	-
12	CWE:502	Deserialization of Untrusted Data	-
13	CWE:190	Integer Overflow or Wraparound	-
14	CWE:287	Improper Authentication	-
15	CWE:798	Use of Hard-coded Credentials	0
16	CWE:862	Missing Authorization	-
17	CWE:77	Improper Neutralization of Special Elements used in a Command ("Command Injection")	-
18	CWE:306	Missing Authentication for Critical Function	-
19	CWE:119	Improper Restriction of Operations within the Bounds of a Memory Buffer	11
20	CWE:276	Incorrect Default Permissions	-
21	CWE:918	Server-Side Request Forgery	-
22	CWE:362	Concurrent Execution using Shared Resource with Improper Synchronization ("Race Condition")	-
23	CWE:400	Uncontrolled Resource Consumption	-
24	CWE:611	Improper Restriction of XML External Entity Reference	-
25	CWE:94	Improper Control of Generation of Code ("Code Injection")	-

### All Other CWE Findings (Excluding Top 25 CWEs)

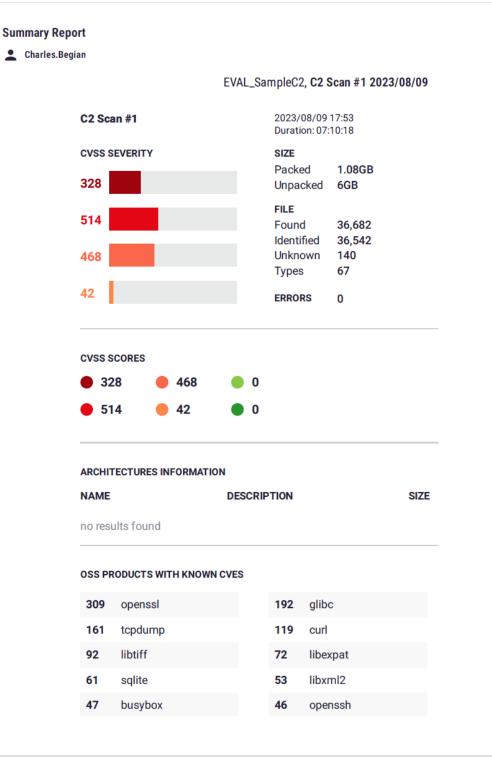
Severity	Score	CWE ID	Name	Instances
Low	2.83	CWE:328	Reversible One-Way Hash	120
Low	2.83	CWE:242	Use of Inherently Dangerous Function	11
Low	2.83	CWE:676	Use of Potentially Dangerous Function	307
Low	2.83	CWE:327	Use of a Broken or Risky Cryptographic Algorithm	120
Low	0.2	CWE:326	Inadequate Encryption Strength	10

www.grammatech.com

Page 1286 / 1292

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 62: C2 Vulnerabilities (mapped to CVEs in the report) (Code Sentry)



# Sample C2 Jarvis Scan Report Excerpts

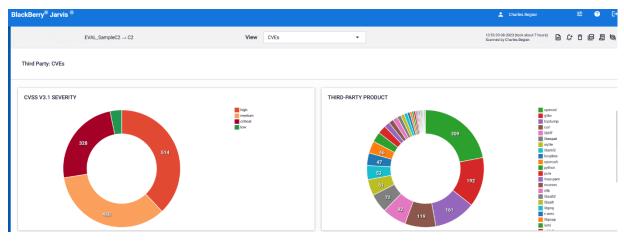
JARVIS

Created: 2023-04-

Figure 63: C2 Scan Overview (Jarvis)

EVALSergieS2 - C2	View Created Intege +		Statistica Statistica Street Distribution Street
mation Lashape: Classified Strings (BETA)			
	Antria em Berger Berg Berg		8 or strate 8 or 8 or
-103			
RENO-RENO	na me Gangar		n); mw
REINST REINST Ange, CE (2016) 2016 and the instance of the Constant and the Constant and the Constant and the Constant and the	6 Information Laskage	THE STATE OF	Franky-6489 -+ 1000.0000.0000.0000.0000.0000.0000.000
RLENO, RESPON	6 biturnation Laskage 6 biturnation Laskage		
REASE FEEDON MARINE, 2014 (STANDARD), THE INFORMATION PROVIDED IN THE INFORMATION OF THE INFORMATION OF THE INFORMATION OF THE AND AND AND AND AND AND AND AND AND AND	s Minimuto Ladiago S Manualia Ladiago Na Ripaño Minimuto Ladiago	TTE Management	Freedge-64.66 1000 0000 0000 0000 0000 0000 000
	د المعنية المع المعنية المعنية المعالمة المعالمة معالمة المعالمة المعالم	PRE PRE Minimum destinations Minimum dest	Г линју 6449 1000 0000 0000 0000 0000 0000 0000
	A constraint A	THE MANAGEMENT OF THE STATE OF	1 * marging data - * ********************************
	Menantication           Maintenantication	THE Ministration of the second secon	Franciska - Vitalisti (1998) 1999 1999 1999 1999 1999 1999 1999
			Francy Sales - Million Statution
			Francyskie – Visitianistianistianistianistianisti Antrophose – Visitianistianistianistianisti Antrophose – Visitianistianistianisti Antrophose – Visitianisti Antrophose – Visitianisti Antrophose – Visitianisti Antrophose (Antrophose) Antrophose – Visitianisti Antrophose Antrophose – Visitianisti Antrophose (Antrophose) Antrophose – Visitianisti Antrophose Antrophose – Visitianisti Ant
	Homestage           Laboration           And a	Pre     Comparison     Comported     Comparison     Comparison     Comparison     Compariso	
		PER     Maximum Control (Control (Contro) (Contro) (Control (Control (Control (Contro) (Control (Contro) (	Francy Same V. Selection State
	Home Starp           Laboration           La	rem     r	
NUMERA NUMBER NUMBER AND DESCRIPTIONS OF AND		POP     Research Construction of Construction     Research Constr	Interprise / wild interpris / wild interprise / wild interprise / wild interpri
		NE           Security Secu	Interplace - Valuational and an address interplace - Valuational and address interplace - Valuation
		NE           Result	Interprise - realizational control and an anti- prior and anti- prior and anti- prior anti-
		EVE     E	Instructional and instrumental and instrumentandinted instrumental and instrumental and instrumental a

Figure 64: C2 Information Leakage (Jarvis)





can Results	Charles.Begian@ 🔻	EVAL_Sa	mpleC2 🗸								
COMPONENT	♦ NAME	\$ DATE	CRITICAL	\$ HIGH	MEDIUM	\$ LOW	PACKED SIZE	UNPACKED SIZE	IDENTIFIED	FOUND	TYPES
				514	468	42	1.08GB	6GB	36542	36682	67
EVAL_Sampl		2023/08/09	328								

Figure 66: C2 CVE Summary by Severity (Jarvis)

Stimestamp	ixtension file info.SHA3-512	file info,file name	file info.ffile info.file type	file info.parent file info.rel; file info.tim; I	has expired	issuer.common inis	suer.col.issuer	om issuer.k	oc.issuer.organization	issuer.organization unit	not after not befo
2023-08-09T17:57:24.918685		557398524d426dcDigiCert High Assurance EV Root CA.			FALSE	DigiCert High Assi U		null	DigiCert Inc	www.digicert.com	20311110C 20061110
2023-08-09717:57:24,918685		b40a000be3a95cf Verisign Class 3 Public Primary Certif			FALSE	null U		null	VeriSien, Inc.	Class 3 Public Primary Certification Authority	20280801219960129
4 2023-08-09T17:57:24.918685	6 017fcec1eb563bfd6786bf03a2f1ceb856			/sample_C2.zip_VSWc2/NVM 2023-08-09T1	FALSE	Secure Global CA U	s null	null	SecureTrust Corport		20291231120061107
2023-08-09717-57:24.918685	2 512fd3739b2ec027c002443560a193640f			/sample_C2.zip_VSWc2/NVV/2023-08-0971	FALSE	self-signed.pythoX			nt Python Software Fo		20241030120141102
6 2023-08-09T17:57:24.918685				/sample_C2.zip_VSWc2/NVN 2023-08-09T1	FALSE	AffirmTrust Prem U		null	AffirmTrust	null	20401231120100129
2023-08-09T17:57:24.918685	5 28bffb2454193b3011ddb1d91f170597b3			/sample_C2.zip_VSWc2/NVN 2023-08-09T1	FALSE	ComSign CA IL	null	null	ComSign	null	20290319120040324
2023-08-09T17:57:24.918685		Wb2e1d75f627dct XRamp Global CA Root.crt		/sample_C2.zip_VSWc2/NVV 2023-08-09T1	FALSE	XRamo Global Cer U		null		www.srampsecurity.com	20350101020041101
2023-08-09T17:57:24.918685		dd8475b9ea16241GlobalSign Root CA - R2.crt		/sample C2.zip VSWc2/NVN 2023-08-09T1	TRUE	GlobalSign n		null	GlobalSign	GlobalSign Root CA - R2	202112150 20061215
0 2023-08-09T17:57:24.918685		372dcab06234b9f Swisscom Root EV CA 2.ot		/sample_C2.zip_VSWc2/NVV_2023-08-09T1	FALSE	Swisscom Root EV cf	null	null	Swisscom	Digital Certificate Services	203106250 20110624
1 2023-08-09T17:57:24.918685				/sample C2.zip VSWc2/NVN 2023-08-0971	FALSE	Secure Certificate G		Salford	Comodo CA Limited		20281231220040101
2 2023-08-09717-57:24.918685		Gadfd0fe1afad18fVisa_eCommerce_Root.crt		/sample_C2.zip_VSWc2/NVW_2023-08-0911	TRUE	Visa eCommerce U		null	VISA	Visa International Service Association	20220624( 20020626
1 2023-08-09T17:57:24.918685		d24fe3156401fc33 Security Communication RootCA2.crt			FALSE	null 3		null		n Security Communication RootCA2	202905290 20090529
4 2023-08-09T17:57:24.918685	4 24ee983e6fbcd56ca770352a2c31236418			/sample_C2.zip_VSWc2/NVW 2023-08-09T1	FALSE	Izenpe.com E		null	IZENDE S.A.	null	203712130 20071213
5 2023-08-09T17:57:24.918685				/sample_C2.zip VSWc2/NVN 2023-08-09T1	FALSE	QueVadis Root C/ B		null	QuoVadis Limited	null	20311124120061124
6 2023-08-09T17-57:24.918685				/sample_C2.zip V5WC2/NVW 2025-08-0911 /sample_C2.zip V5WC2/NVW 2023-08-0911	FALSE	Certum Trusted N P	null	null		e Certum Certification Authority	20461006( 20111006
7 2023-08-09117:57:24.918685		1c8062f95292e2d E-Tugra Certification Authority.ort		/sample_C2.cip_VSWc2/NVW 2023-08-0911 /sample_C2.cip_VSWc2/NVW 2023-08-0911	TRUE	E-Tuera Certificat T		Ankara		In E-Tuera Sertifikasion Merkezi	20230303120130305
E 2023-08-09T17:57:24.918685				/sample_C2.zip_V5Wc2/NVN 2023-08-0971	FALSE	Microsec e-Szienc H			et Microsec Ltd.	null	20291230120090616
9 2023-08-09T17:57:24.918685				/sample C2.zip VSWc2/NVN 2023-08-09T1	TRUE	TÄDBÄ'TAK UEKATI	t null			e Ulusal Elektronik ve Kriptoloji AraÅ?tätrma Er	
0 2023-08-09117-57:24,918685		7a9ec6290a4bd0c QuoVadis Root CA 2 G3.ort		/sample_C2.zip_V5Wc2/NVW 2023-08-0971	FAISE	OunVadis Boot C/B		null		null	20420112120120112
2023-08-09117-57:24,918685	9 4a980ec8d576db0919138ea8df2a1a0d6			/sample_C2.rip_V3Wc2/NVW 2023-08-0911 /sample_C2.rip_V3Wc2/NVW 2023-08-0911	TRUE	Autoridad de Cert V		@suCaracas		<ul> <li>Superintendencia de Servicios de Certificacion</li> </ul>	
2 2023-08-09117-57:24.918685		3552294bb9e4be1TURKTRUST Certificate Services Provid			TRUE	TÅrefixTRUST Flei T		Ankera	TĂGERKTRUST BILEI		20171222120071225
2023-08-09117:57:24.918685				/sample_C2.zip VSWC2/NVV 2023-08-0911 /sample_C2.zip VSWC2/NVV 2023-08-0911	FALSE	SwissSign Gold C/ C		null	SwissSign AG	null	203610250 20061025
4 2023-08-09T17:57:24.918685	3 2cf86df132ef5efe584868e2c8d7108804c			/sample_C2.zip VSWC2/NVN 2023-08-09T1	FALSE	CA Disig Root R2 SI			ra Disig a.s.	null	20420719(20120719
5 2023-08-09T17:57:24.918685		Reb5d8dfe84b0arVerisign Class 1 Public Primary Certif			FALSE	null U		null	VeriSien, Inc.	Class 1 Public Primary Certification Authority	20280802219960129
6 2023-08-09117:57:24.918885				/sample_C2.rip_V5Wc2/NVV 2023-08-0911 /sample_C2.rip_V5Wc2/NVV 2023-08-0911	FALSE	COMODO Certific G		Salford			20291231220061200
7 2023-08-09117:57:24.918685		f7174ab2f2735c2/SecureSian RootCA11.ort		/sample_C2.rip_V5Wc2/NVW 2023-08-0911 /sample_C2.rip_V5Wc2/NVW 2023-08-0911	FALSE	SecureSign RootC JI	null	null	Japan Certification		202904080 20090408
2023-08-09117:57:24.918685 8 2023-08-09117:57:24.918685				/sample_C2.tip VSWc2/NVW 2023-08-0911 /sample_C2.zip VSWc2/NVW 2023-08-0911	FALSE	AAA Certificate SrG		Salford			20281231220040101
9 2023-08-09117-57:24.918685	I fc8Jea0777b01af0be67128a2c2b77975d			/sample_C2.zip_V3WC2/NVW 2023-08-0911 /sample_C2.zip_VSWC2/NVW 2023-08-0911	FALSE	GlobalSign Root CB	i null	null	GlobalSign me-sa	Root CA	20280128119980901
0 2023-08-09117-57:24.918685	6 e16230f500fab57e1485b3fo428833b43a			/sample_C2.pp vswc2/nvvv 2023-08-0911 /sample_C2.pp vSwc2/NVV 2023-08-0911	FALSE	SecureTrust CA U		null	SecureTrust Corport		20291231120061107
0 2023-08-09117:57:24.918685	6 e1023030018037e14630304288330439 5 354d278f2310b236b64afdc7d530950870			/sample_C2.pp_VSWc2/NVW 2023-08-0911 /sample_C2.pp_VSWc2/NVW 2023-08-0911	FALSE	testroot C		null	zte	null	20291231120061107 20280621120180621
2 2023-08-09117:57:24.918685					FALSE	Certification Auth C		null	WoSign CA Limited		
3 2023-08-09117:57:24.918685	3 d8f1d5e180a0e7703da6efa69a21f70834	3255aacd5f6f13drAffirmTrust_Networkine.ort		/sample_C2.zip VSWc2/NVN 2023-08-09T1	FALSE	AffirmTrust Netw U			AffirmTrust	nul	20390808C20090808 20301231120100129
		beaaf3f3ffe1eeb/GlobalSign_Root_CA + R3.crt		/sample_C2.zip VSWc2/NVN 2023-08-09T1	FALSE			null		GlobalSign Root CA - R3	
4 2023-08-09117:57:24.918685 5 2023-08-09117:57:24.918685				/sample_C2.zip VSWc2/NVN 2023-08-09T1	FALSE	GlobalSign n Staat der Nederla N		null	GlobalSign Staat der Nederlans		20290318120090318 20281113220131114
	5 a86e6781ff2bcb73244cfae0e8a0758952	89ab44a2128f441 Staat_der_Nederlanden_Root_CA - G3			TRUE			null	staat oer Nederlant	e null	
6 2023-08-09117:57:24.918685 7 2023-08-09117:57:24.918685	1 a51e56a9f581e11dc332711c1d8210e0dd			/sample_C2.zip VSWc2/NVV 2023-08-09T1 /sample_C2.zip VSWc2/NVV 2023-08-09T1	TRUE	testroot C localhost X			at Python Software Fo		20200621120180621 20201005720101008
2023-08-09117-57:24.918685								castle A			
		Adoc7d137ec863f9 Verisign_Class_3_Public_Primary_Certif			FALSE	VeriSign Class 3 P U			VeriSign, Inc.	VeriSign Trust Network	20360716219991001
© 2023-08-09T17:57:24.918685		3107fd45faa20352 GeoTrust_Primary_Certification_Author			FALSE	GeoTrust Primary U	s null	Itun	GeoTrust Inc. Unizeto So. z o.o.	nul	20360716220061127
0 2023-08-09T17:57:24.918685	1 d1ac1bb0f09ef039b93ebbdc6cc20c4663			/sample_C2.zip VSWc2/NVV 2023-08-09T1				null			20270611120020611
1 2023-08-09117:57:24.918685				/sample_C2.zip VSWc2/NVV 2023-08-0971	TRUE	Root CA Generalit E		nuti	Generalitat Valenci		20210701120010706
2 2023-08-09T17:57:24.918685				/sample_C2.zip VSWc2/NVW 2023-08-09T1				null		e T-Systems Trust Center	20331001220081001
3 2023-08-09T17:57:24.918685		ad115aabBed5b9 DigiCert_Trusted_Root_G4.crt		/sample_C2.zip VSWc2/NVW 2023-08-09T1	FALSE	DigiCert Trusted FU		null	DigiCert Inc	www.digicert.com	20380115320130803
4 2023-08-09117:57:24.918685		I6edaa487e6c7b7 CertinomisRoot_CA.crt		/sample_C2.zip VSWc2/NVW 2023-08-0971	FALSE	Certinomis - Root Fl		null	Certinomis	0002 433998903	20331021(20131021
5 2023-08-09T17:57:24.918685		d3f602242c75336cTWCA_Root_Certification_Authority.crt			FALSE	TWCA Root Certif T		null	TAIWAN-CA	Root CA	20301231120080828
6 2023-08-09T17:57:24.918685		tc2cf9ee40a1f194:COMODO_ECC_Certification_Authority.			FALSE	COMODO ECC Cer G		Salford	COMODO CA Limite		20380118720080306
7 2023-08-09T17:57:24.918685				/sample_C2.zip VSWc2/NVM 2023-08-09T1	FALSE	AC Raã-z CerticĂi C		null	Sociedad Cameral d		20300402220061127
8 2023-08-09117:57:24.918685	0 4de6c6bc3c36dc159d6d69a2480ee31aa			/sample_C2.zip_VSWc2/NVV/2023-08-09T1	TRUE	brutus.neuronio.(P		s@ilLisboa	Neuronio, Lda.	Desenvolvimento	19961005(19960905)
0 2023-08-09T17:57:24.9186R5		sff77f2cb99o531acOISTE WISeKey Global Root GB CA.cr			FALSE	OISTE WISeKey GIC	- null	null	WISeKey	<b>OISTE Foundation Endorsed</b>	20391201120141201

Figure 67: C2 Certificates report (Jarvis)

A	8	c	DE	F.:	G	н I	1	К.	L M	N	0	a a	5	U	V	W
	certain				v cve.cvss.v2.vector	cve.cvss.v cve.cvss.v						sescri eve.name		wd_info.update.cve.nvd_in		we.problem_type
<= 2.32	TRUE	libresolv	2.1 fow		AV:L/AC:L/Au:N/C:N/EN/A:P	5.5 medium	TRUE		5.5 medium	FALSE	CVSS:3.1/AV:L/AC:L/PR:L/UEN/S:U/C:N/EN//The		2/26/2021	10/28/2022 https://nvi		
[2.24, 2.26]	TRUE	libresolv	7.5 high	FALSE		9.8 critical	FALSE		9.8 critical	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/The		2/2/2018	8/24/2020 https://nvi		
< 2.26	TRUE	libresolv	5 medium	FALSE		5.3 medium	TRUE		5.3 medium	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/ Cert		10/14/2010	3/31/2020 https://nvi		
<= 2.26	TRUE	libresolv	7.2 high	FALSE		7.8 high	FALSE		7.8 high	TRUE	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/AIngl		1/31/2018	10/3/2019 https://nvi		
<= 2.29	TRUE	libresolv	7.5 high	FALSE		9.8 critical	TRUE	CV55:3.0/.	9.8 critical	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/ In th		2/26/2019	6/13/2022 https://nvi		
<2.32.0	TRUE	libresolv	2.1 low	FALSE		5.5 medium	TRUE		5.5 medium	FALSE	CVSS:3.1/AV:L/AC:L/PR:L/UEN/S:U/C:N/EN/#The		3/4/2020	11/10/2022 https://nvi		
<= 2.26	TRUE	libresolv	7.5 high	FALSE		9.8 critical	FALSE		9.8 critical	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:H/EH/An in		2/1/2018	8/24/2020 https://nvi		
<= 2.26	TRUE	libresoly	7.5 high	FALSE		9.8 critical		CV55:3.0/.	9.8 critical	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/The		10/22/2017	6/20/2018 https://nvi		
[1.0.2, 1.0.25], [1.1.0, 1.1.08], [1.1	TRUE	liberypto	1.9 low	FALSE		3.3 low	FALSE		3.3 low	TRUE	CVSS:3.1/AV:L/AC:L/PR:L/UEN/S:U/C:N/EL/A:N	CVE-2019-1552	7/30/2019	12/13/2022 https://nvi		
[1.0.2, 1.0.25], [1.1.0, 1.1.08], [1.1	TRUE	libcrypto	4.3 medium	FALSE		3.7 low	TRUE	CV55:3.0/.	3.7 low	FALSE	CVSS:3.1/AV:N/AC:H/PR:N/UEN/S:U/C:L/EN/In sil		9/10/2019	7/31/2021 https://nvi		
[ [1.0.2, 1.0.2m], [1.1.0, 1.1.0g]		liberypto	4.3 medium	FALSE		5.9 medium	TRUE		5.9 medium	FALSE	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	CVE-2017-3738	12/7/2017	8/19/2022 https://nvi		
[7.19.4, 7.65.3]	TRUE	libcurl	7.5 high	FALSE		9.8 critical	TRUE		9.8 critical	FALSE	CV\$5:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:H/EH/Heat		9/16/2019	11/3/2021 https://nvi		
4 [7.33.0, 7.78.0]	TRUE	libourt	5 medium	FALSE		7.5 high	TRUE		7.5 high	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:N/I:N/IIbcu		8/5/2021	1/5/2023 https://nvi		
5 [7.16.4, 7.84.0]	TRUE	libcuri	4.3 medium	FALSE	AV:N/AC:M/Au:N/C:P/I:N/A:N	5.9 medium	TRUE		5.9 medium	FALSE	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N Whe	n curi CVE-2022-32208	7/7/2022	1/5/2023 https://nvi		
6 [7.20.0, 7.59.0]	TRUE	libcurl	6.4 medium	FALSE	AV:N/ACIL/Au:N/CIP/EN/ASP	9.1 critical	FALSE	CV55:3.0/.	9.1 critical	TRUE	CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/C:H/EN/out	versic CVE-2018-1000301	5/24/2018	10/3/2019 https://nvi	d.nist.gov/vuln, C	WE-125
7 [7.7, 7.78.0]	TRUE	libcurl	5 medium	FALSE	AV:N/AC:L/Au:N/C:P/EN/A:N	5.3 medium	TRUE	CV55:3.0/.	5.3 medium	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:L/I:N/ curl	suppc CVE-2021-22925	8/5/2021	1/5/2023 https://net	d.nist.gov/vuln, C	WE-908
[7.1, 7.57.0]	TRUE	libcuri	5 medium	FALSE	AV:N/AC:L/Au:N/C:P/I:N/A:N	9.8 critical	TRUE	CV55:3.0/-	9.8 critical	FALSE	CV55:3.1/AV:N/AC:L/PR:N/U:N/5:U/C:H/I:H/IIbeu	rl 7.1 CVE-2018-1000007	1/24/2018	6/13/2022 https://nvi	d.nist.gov/vuln/d	Jetail/CVE-2018-1
9 < 7.83.1	TRUE	libcurl	5 medium	FALSE	AV:N/AC:L/Au:N/C:N/I:N/A:P	7.5 high	TRUE	CV55:3.0/.	7.5 high	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:N/I:N/Ilbcu	rl prc:CVE-2022-27781	6/2/2022	1/5/2023 https://nv	I.nist.pov/vuln, C	WE-835
<8.1.0	TRUE	libcurl	2.6 low	TRUE	AV:N/AC:H/Au:N/C:P/I:N/A:N	3.7 low	TRUE	CVSS:3.0/.	3.7 low	FALSE	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/An in	form CVE-2023-28322	5/26/2023	6/16/2023 https://net	d.nist.gov/vuln/d	Jetail/CVE-2023-2
	TRUE	libncurse	5 medium	FALSE	AV:N/AC:L/Au:N/C:N/I:N/A:P	7.5 high	FALSE	CV55:3.0/.	7.5 high	TRUE	CV55:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/In no	urses CVE-2017-11113	7/8/2017	5/6/2019 https://nvi	f.nist.gov/vuln,C	WE-476
6	TRUE	libncurse	4.3 medium	FALSE	AV:N/AC:M/Au:N/C:N/EN/A:P	6.5 medium	FALSE	CV55:3.0/.	6.5 medium	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/ULR/S:U/C:N/I:N/Ther	e is aiCVE-2017-13734	8/29/2017	10/21/2018 https://mw	f.nist.gov/vuln,C	WE-119
< 7.2	TRUE	ssh-	7.5 high	FALSE	AV:N/ACIL/Au:N/C:P/LP/A:P	9.8 critical	TRUE	CV55:3.0/i	9.8 critical	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/ULN/S:U/C:H/I:H/The	lient CVE-2016-1908	4/11/2017	12/13/2022 https://nv	d.nist.eov/vuln.C	WE-287
4 40 6.5	TRUE	ssh-	5.8 medium	FALSE	AV:N/AC:M/Au:N/C:P/I:P/A:N	4.9 medium	FALSE	CV55:3.0/.	4.9 medium	TRUE	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A sshd	in Oc CVE-2014-2532	3/18/2014	7/19/2018 https://nv	f.nist.pov/vuln.C	WE-264
5 <= 6.9	TRUE	ssh-	1.9 low	FALSE	AV:L/AC:M/Au:N/C:N/EP/A:N	4 medium	TRUE	CV55:3.0/.	4 medium	TRUE	CVSS:3.1/AV:L/AC:L/PR:N/UEN/S:U/C:N/EL//The	monitCVE-2015-6563	8/24/2015	12/13/2022 https://nw	finist.eov/vuln.C	WE-20
5 cu 7.3	TRUE	ssh-	6.9 medium	FALSE	AV:L/AC:M/Au:N/C:C/EC/A:C	7 high	FALSE	CV55-2.0/.	7 high	TRUE	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H//sshd		1/5/2017	12/13/2022 https://nv		
7 <= 7.3	TRUE	ssh-	7.5 high	FALSE		7.3 high	FAISE	CV55:3.0/	7.3 high	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/4Untr		1/5/2017	12/13/2022 https://nv		
<= 2.9.2		libxml2	5 medium	FALSE		5.3 medium	TRUE		5.3 medium	TRUE	CVSS:3.1/AV:N/AC:U/PR:N/UI:N/S:U/C1/I:N/ Heat		12/15/2015	2/13/2023 https://ne		
<2.9.3	TRUE	libxml2	7.5 high	FALSE		9.8 critical	TRUE	CV55:3.0/.	9.6 critical	FALSE	CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/C:H/EH/The		4/11/2016	2/26/2020 https://nv		
□ <= 2.9.1	TRUE	libxml2	5 medium	FAISE		7.5.high		CV55:3.0/.	7.5 high	TRUF	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/The		5/16/2016	11/4/2017 https://nv		
c= 2.9.2	TRUE	libxml2	5 medium	FALSE		5,3 medium	TRUE	CV55:3.0/	5.3 medium	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/ The		12/15/2015	9/14/2017 https://ne		
2 = 2.9.1	TRUE	libxml2	5 medium	FALSE		7.5 high		CV55:3.0/	7.5 high	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:N/EN/The		5/16/2016	11/4/2017 https://nv		
<2.9.4	TRUE		9.3 critical	FALSE		7.8 high		CV55:3.0/.	7.8 high	TRUE	CVSS:3.1/AV:J/AC:J/PR:N/UIR/5:U/C:H/IH//Heat		5/20/2016	3/25/2019 https://nv		
6 c= 2.9.6	TRUE	libxml2	4.3 medium	FALSE		5.5 medium	FALSE		5.5 medium	TRUE	CVSS:11/AV1/AC1/PR:N/UER/SU/C:N/EN//The		5/20/2016	3/25/2019 https://nv		
c=2.9.4	TRUE	libxml2	7.5 high		AV:N/AC:L/Au:N/C:P/I:P/A:P	9.8 critical	FALSE		9.8 critical	TRUE	CVSS:3.1/AV:N/AC:U/PR:N/UEN/S:U/C:H/EH/A fla		2/19/2018	3/18/2018 https://nv		
~2.9.2	TRUE	libxml2	6.4 medium	FALSE		6.5 medium	TRUE	CV55:3.0/.	6.5 medium	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:L/I:N/ The		12/15/2015	9/14/2017 https://nv		
7 <= 2.9.2	TRUE	libxmi2	5 medium	FALSE		5.3 medium	TRUE	CV55:3.0/.	5.3 medium	TRUE	CVSS:3.1/AV:N/AC:L/PR:N/U:N/S:U/C:N/I:N/Heat		12/15/2015	2/12/2023 https://nv		
<2.9.10	TRUE	libxml2	5 medium	FAISE		7.5 high	TRUE	CV55:3.0/	7.5 high	FAISE	CVSS:3.1/AV:N/AC:U/PR:N/UEN/S:U/C:N/EN/xmlP		12/24/2019	7/21/2021 https://ne		
0 c= 2.9.2	TRUE	libxml2	5 medium	FALSE		5.3 medium	TRUE	CV55:3.0/.	5.3 medium	TRUE	CVSS:3.1/AV.N/AC:L/PR:N/U:N/S:U/C:N/I:N/Heat		12/15/2015	2/12/2023 https://nv		
G 3.31.1	TRUE		7.5 high			9.8 critical	TRUE		9.8 critical	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/UEN/S:U/CH/IH/IN SC		4/9/2020	4/8/2022 https://nv		
<3.32.0	TRUE		4.4 medium	FALSE		7 high	TRUE	CV55:3.0/.	7 high	FALSE	CVSS3.1/AV://aC:H/PR://USR/SU/C:H/I:H/I inst		5/27/2020	5/13/2022 https://nv		
< 3.320 (~ 3.31.1	TRUE	libsqlite		FALSE			TRUE	CV55:3.0/.	7.5 high	FALSE	CVSS3.1/AV3/AC1/PR:N/UEN/S:U/C:H/H074ER/ CVSS3.1/AV.N/AC1/PR:N/UEN/S:U/C:H/H074ER/		4/9/2020	4/8/2022 https://nv		
		libsqlite	5 medium			7.5 high										
[3.8.5, 3.29.0]	TRUE	libsqlite	4.3 medium	FALSE		6.5 medium	TRUE		6.5 medium	FALSE	CVSS:3.1/AV:N/AC:L/PR:N/U:R/5:U/C:N/I:N/ In S0		9/9/2019	3/23/2023 https://nvi		
[1.0.2, 1.0.25], [1.1.0, 1.1.08], [1.1	TRUE	liberypto	1.9 low	FALSE		3.3 low		CV55:3.0/	3.3 low	TRUE	CVSS:3.1/AV:L/AC:L/PR:L/UEN/S:U/C:N/EL/A:N	CVE-2019-1552	7/30/2019	12/13/2022 https://mv		
5 [1.0.2, 1.0.2k], [1.1.0, 1.1.0c]	TRUE	liberypto	2.6 low	FALSE		5.9 medium	TRUE	CV55:3.0/.	5.9 medium	FALSE	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	CVE-2016-7055	5/4/2017	9/1/2022 https://nvi		
5 [1.0.2b, 1.0.2m]		liberypto	4.3 medium	FALSE		5.9 medium		CV55:3.0/	5.9 medium	TRUE	CV55:3.1/AV:N/AC:H/PR:N/UI:N/5:U/C:H/I:N/A:N	CVE-2017-3737	12/7/2017	10/3/2019 https://nv		
[1.0.2, 1.0.2zd], [1.1.0, 1.1.1n], [3	TRUE	liberypto	5 medium	FALSE		7.5 high	TRUE	CV55:3.0/	7.5 high	FALSE	CVSS:3:1/AV:N/AC:L/PR:N/UEN/S:U/C:N/EN/A:H	CVE-2022-0778	3/15/2022	11/9/2022 https://nvi		
[1.0.2, 1.0.2p], [1.1.0, 1.1.0i], 1.1.	TRUE	liberypto	4.3 medium	FALSE		5.9 medium	TRUE	CV55:3.0/.	5.9 medium	FALSE	CVSS:3.1/AV:N/AC:H/PR:N/ULN/S:U/C:H/I:N The		10/30/2018	8/29/2022 https://nvi		
[1.0.2, 1.0.2zh], [1.1.1, 1.1.1u], [3	TRUE	liberypto	7.8 high	TRUE	AV:N/AC1/AurN/C:N/EN/A-C	7.5 high	TRUE	CV\$5:3.0/i	7.5 high	FALSE	CV55:3.1/AV:N/AC:L/PR:N/UI:N/5:U/C:N/I:N/A	CVE-2023-0464	3/22/2023	6/8/2023 https://nvi	finist.cov/yulo C	WE-295

Figure 68: C2 CVEs (Jarvis)

6 A   B	c	0 E F		н	1	1	K L M		0 A8	AC	AD	M.	AF	AG AI A	AL AL	AM	AN
@timesta domain	file_info.MD5	file_info_file_info_file_i			file_info.extension		file_info.ffile_info.ffile_in				le_info.sfil	e_info.s					
2023-08-0t openssh.com	255211d11abc09605bc93c6931863f71	d5cd0a9fe433ea6bc17ad55	2da/0aecc1ccb	FALSE		ssh-keysign	ELF 64-bit /sample_(ELF	RegularFil 201	8-07-2 /sample	(VSWc2/N)	0	33,188	432,528	0 2023-08-0: REG	umac-1	28-ef90a9d0-u	mac-128-etm@openssh.com
2023-08-0t openssh.com	255211d11abc09605bc93c6931863f71	d5cd0a9fe433ea6bc17ad55		FALSE		ssh-keysign	ELF 64-bit /sample_(ELF	RegularFil 201	8-07-2/sample	LVSWc2/N	0	33,188	432,528	0 2023-08-0 REG	hmac-si	ha ef90a9d0- h	mac-sha1-etm@openssh.com
2023-08-0 openssh.com	255211d11abc09605bc93c6931863f71	d5cd0a9fe433ea6bc17ad55	i2def@eecclccb	TRUE		ssh-keysign	ELF 64-bit /sample_(ELF	RegularFil 201	8-07-Z/sample	tusr/libexc	1,000	33,225	432,528	1,000 2023-08-0 REG	hmac-si	ha ef90a9d0- h	mat-sha1-etm@operissh.com
2023-08-0 openssh.com	255211d11abc09605bc93c6931863f71	d5cd0a9fe433ea6bc:7ad55	i2da/Gaecc1ccb	FALSE		ssh-keysign	ELF 64-bit /sample_(ELF	RegularFil 201	3-07-2/sample	(VSWc2/N)	0	33,188	432,528	0 2023-08-0 REG	hmac-m	nd: ef90a9d0- h	mac-md5-etm@openssh.com
2023-08-0t openssh.com	255211d11abc09605bc93c6931863f71	d5cd0a9fe433ea6bc17ad55	2dai0aecc1ccb	TRUE		ssh-keysign	ELF 64-bit /sample_(ELF	RegularFil 201	8-07-2 /sample	(usr/libexe	1,000	33,225	432,528	1,000 2023-08-0 REG	hmac-m	idt ef90a9d0- h	mac-md5-96-etm@openssh.com
2023-08-0 python.org	498fed720823d1a3d2c883dc00d57e88	aaf716cd3 b1e57faef e8338	R0c95 ba3e5d82i	TRUE	-124	_aboutpy	Python sci/sample_(PYTHO	N_!RegularFil 201	9-03-0 /sample	(V5Wc2/N)	0	33,188	817	0 2023-08-0 REG	cryptog	raj ef90a9d0- cr	yptography-dev@python.org
2023-08-0 zte.com.cn	a3cf9a76ca9ea55f4f3c6f538ccb6d33	ee44f65dt f75259c06 00afa	1o4f17f2b79685	TRUE	-yang	PucchConfigCommon.yan	UTF-8 Unit/sample_(UTF_8	TE: RegularFil 201	8-05-0 /sample	(VSWc2/N	0	33,188	4,832	0 2023-08-0 REG	101347	72 ef90a9d0- 1	0134772@zte.com.cn
2023-08-01zte.com.cn	a3cf9a76ca9ea5564f3c6/538ccb6d33	ee44f65dt f75259c06 00afa	1o4f17f2b79685	FALSE	.yang	PucchConfigCommon.yan	UTF-8 Unix/sample_(UTF_8	TEI RegularFil 201	8-05-0 /sample	(VSWc2/N)	0	33,188	4,832	0 2023-08-0 REG	2281	50 ef90a9d0-0	1228160@zte.com.cn
2023-08-01 zte.com.cn	a3cf9a76ca9ea55f4f3c6f538ccb6d33	ee44/65dt 175259c06 00afa	10411712579685	TRUE	.yang	PutchConfigCommon.yan	UTF-8 Unix/sample_(UTF_8	TEI RegularFil 201	9-03-1 /sample	(VSWc2/N	0	33,188	4,832	0 2023-08-0 REG	2281	60 ef90a9d0-0	1228160@zte.com.cn
2023-08-0 gmail.com	22daf359b2b466bbfef6e08f7cb2fa68	64b67cear da2a7cf53 de013	54e5 ab07d775i	TRUE	-94	file.py	Python sci/sample_(PYTHO	N_!RegularFil 201	9-03-0 /sample	(VSWc2/N	0	33,188	19,215	0 2023-08-0: REG	robeyp	oir ef90a9d0- ro	beypointer@gmail.com
2023-08-0' arbash-meinel.com	43252c50babcaf4cf5188c8d76b2aa28	134a96f2d 0560964a8 f2977	805c 48a47762t	FALSE	-PY	win_pageant.py	Python sci/sample_(PYTHO	N_!RegularFil 201	9-03-0 /sample	(VSWc2/N)	0	33,188	4,210	0 2023-08-0 REG	john	ef90a9d0-jo	hn@arbash-meinel.com
2023-08-01zte.com.cn	32678cef93edc35531dc5bee3b667c49	dcf22312d04b3379d1ccaec	4268 0ab390d1/	FALSE	.yang	action-bum-aisg.yang	UTF-8 Unix/sample (UTF 8	TEI RegularFil 201	8-05-0 /sample	(VSWc2/N	0	33,188	12,865	0 2023-08-0 REG	zhang h	er ef90a9d0-zi	nang heng5@zte.com.cn
2023-08-0r zte.com.cn	32678cef93edc35531dc5bee3b667c49	dcf22312d04b3379d1ccaec	4268 Oab390d1/	TRUE	yang	action-bum-aisg.yang	UTF-8 Unix/sample (UTF 8	TEI RegularFil 201	9-07-3/sample	(VSWc2/N)	0	33,188	12,865	0 2023-08-0 REG	zhang.h	er ef90a9d0- zi	hang.heng5@zte.com.cn
2023-08-0 zte.com.cn	32678cef93edc35531dc5bee3b667c49	dcf22312d04b3379dfocaec	4268 Oab390d1/	TRUE	veng	action-bum-aisg.yang	UTF-8 Univ/sample (UTF 8	TE: RegularFil 201	8-05-0 /sample	(model/bu	0	33.188	12.865	0 2023-08-0 REG	zhang.h	er ef90a9d0- zi	rang.heng5@zte.com.cn
2023-08-0 softhome.net	69a0a828ccebf7b78b7de209afbace15	a3654c827 acc274cc1/51388	isde: fb5088ff8/	FALSE	-94	test_optparse.py	Python sci/sample_(PYTHC	N_!RegularFil 201	3-03-0 /sample	(VSWc2/N)	0	33,188	62,721	0 2023-08-0 REG	taradin	o ef90a9d0-ta	radino@softhome.net
2023-08-0 softhome.net	69a0a828ccebf7b78b7de209afbace15	a3654c827acc274cc1(51388	Isde: fb5088ff8(	TRUE	-PV	test optparse.py	Python sci/sample (PYTHO	W !RegularFil 201	9-03-0 /sample	(VSWc2/N)	0	33,188	62,721	0 2023-08-0 REG	taradim	ef90a9d0-ta	radino@softhome.net
2023-08-0: python.org	12591a2ed4aa2174e461ab7ca6bbb18c	771635abi 71d66ae4i d7011	7300 90ad52291	FALSE	-54	application.py	Python sci/sample (PYTHO	N !RegularFil 201	9-03-0 /sample	(V5Wc2/N)	0	33,188	1.292	0 2023-08-0 REG	email-s	ig ef90a9d0-e	mail-sig@python.org
2023-08-0 example.com	f55bcbec3b20b0eeb5284ae93d2570b	d f5ca2513d 3ea4d415-52c73	fcc3;20670ab3t	FALSE	.txt	mgg 38.txt	MIME enti/sample (TEXT )	FILE RegularFil 201	9-03-0 /sample	(VSWc2/N	0	33.188	2,649	0 2023-08-0 REG	20592.1	02 ef90a9d0- 2	1592.1022586929.4@example.com
2023-08-01 zte.com.cn	8bca3d70140d221e12ddd86d025e804	9 7aaafe3b1 477af1292 4b6d	ana b4f84d0c8	TRUE	.vin	action-bum-smp.vin	XML1.0 di/sample (XML	RegularFil 201	9-07-2 /sample	(V5Wc2/N)	0	33.188	2,712	0 2023-08-0 REG	zhai.wa	nt ef90a9d0- zi	na), wantena @zte.com.cn
2023-08-0 python.org	41bt7569e9bc0afafb48c9e4c00e941d	2106a4dc3 1e98e8fei 37da3	42c5 cf11248ce	FALSE	pyc	six.pyc	python 2.1/sample (PYTHO	N (RegularFil 201	9-07-3/sample	(VSWc2/N)	0	33,188	30,809	0 2023-08-0 REG	benjam	in ef90a9d0-b	enjamin@python.org
2023-08-0t openssh.com	156a2cdf36281f27a649755e54a794b8	5e399917ccf21f2e0d 8dfcb	0c35 cbab1d0fe	FALSE	exe		ELF 64-bit /sample (ELF		9-03-0 /sample		0	33.188	7.051.072	0 2023-08-0 REG			ardlink@openssh.com
2023-08-0 openssh.com	4e2afd3dbe7449da59d89497d400c2ac	fb1e4406c9b961ed1;a9d77	217; c72bb1674	TRUE		ssh-add	ELF 64-bit /sample (ELF	RegularFil 201	8-07-2 /sample	iusr/bin/st	1.000	33,261	329.936	1.000 2023-08-0 REG	ssh-rsa-	ce ef90a9d0-st	h-rsa-cert-v01@cpenssh.com
2023-08-0' openssh.com	4e2afd5dbe7449da59d89497d400c2ac	fb1e4406c9b961ed1;a9d77	2173 c72bb1674	TRUE		ssh-add	ELF 64-bit /sample (ELF	RegularFil 201	8-07-2/sample	(usr/bin/st	1.000	33.261	329.936	1.000 2023-08-0 REG	ecdsa-s	ha ef90a9d0- e	odsa-sha2-nisto521-cert-v01@openssh.
2023-08-01 222.org	fde67c346d38a0P38d83/fkr9357dPa6	1474bcfe805d5e533/11795	aa6/i5df6abbc6	TRUE	.txt	msg 02.txt	ASCII text /sample (TEXT )				0	23.188	2.812	0 2023-08-0 REG	pop-res	our ef90a9d0- p	pp-request@zzz.org
2023-08-0"222.org	fde67c346d38a0f96d83f9c9357df9a6	1474bcfe805d5e533/11795	aafri Sdffabbre	FALSE	.txt		ASCII text /sample (TEXT )				0	33,188	2.812	0 2023-08-07 REG	900	ef90a9d0-P	
2023-08-01222.org	fde67c346d38a0f98d83f9c9357df9a6	1474bcfe805d5e533i11795		TRUE	.txt		ASCII text /sample (TEXT )					33,188	2,812	0 2023-08-07 REG	Ppp	ef90a9d0- P	
2023-08-01 nerd sh	83ab3674cf45bf15998e86af15e18b90			FALSE	-PV		Python sci/sample (PYTHO				0	33.188	11.038	0 2023-08-0 REG	reek	ef90a9d0-g	
2023-08-01 nerd.sh	83ab3674cf45bf15998e86af15e18b90	9312e156c6F2cb18bebe11	iff1c dectifica0:	TRUE	.cv		Python so/sample (PyTHO				0	33,188	11.038	0 2023-08-0 REG	peek	ef90a9d0-@	
2023-08-0 uk.ibm.com	55f9dce4bc9aca58e3e8ee3bc9754d57			FALSE	decTest		ASCII text /sample (ASCII					33,188	9,703	0 2023-08-0 REG	mfc		fc@uk.ibm.com
2023-08-0 dom.com	b37af238b9e67daf06643519bf6e2855			FALSE	-94		Python sci/sample (PYTHC					33.188	18.562	0 2023-08-07 REG	person		erson@dom.com
2023-08-0 thyrsus.com	71f83c0425eafa4e877ca495265efd5b	e 20f63239 c006a0048 e 2f83	b7d1c8bbed6b	FALSE	-DV		Python sci/sample (PYTHO				0	33,188	34.558	0 2023-08-07 REG	esr	efstalidt e	ur@thyrsus.com
2023-08-01 lemburg.com	89c7d5fe43438438efbd50041e3fba00	rf2090he77reedatily338ar	572c ed9:995er	FALSE	-PY		Python sci/sample (PYTHO					33,188	2.422	0 2023-08-0 REG	mal		al@lemburg.com
2023-08-0' example.com	2221c6e3208b7dec2476b7ea4235e1bc			FALSE	out		ELF 64-bit /sample (ELF		9-03-01/sample				5,635,880	0 2023-08-0 REG	ftp		p@example.com
2023-08-0"zte.com.cn	7208aed0a220fe378941dba6262a7045			FALSE			ASCII text /sample (ASCII		9-07-2 /sample			33.188	2,268	0 2023-08-0 REG			hang zelian@zte.com.cn
2023-08-01 example.org	fbebd719ce503b382e1f27082b323277			FALSE	.conf		ASCII text /sample (CONFI					33,188	5.517	0 2023-08-0 REG	me		e@example.org
2023-08-0: gmail.com	49cb6c241ff67bd51ef5dd73e3626736			TRUE	-PY		Python sci/sample (PYTHO					33,188	1.865	0 2023-08-0 REG			tingof@gmail.com
2023-08-0 python.org	47fb7b6f178872b76f1dbe273bc98dbd			FALSE	egg-info		ASCII text /sample (ASCII					33.188	1.556	0 2023-08-0 REG			thon-dev@python.org
2023-08-0 stuartbishop.net	a53dbbd7bcdee6fc0a116a5f7883b29c			TRUE	lison		JSON data/sample (PYTHC					33,168	906	0 2023-08-0 REG			uart@stuartbishop.net
2023-08-0 python.org		d3e3b419 808427b6: 78f69		FALSE	.51		Python so/sample (PYTHO					33.158	50,769	0 2023-08-0 REG			thon-list@ovthon.org
2023-08-0 nongnu.org	db33c03b50288e807f027b618fcdcb73			FALSE			ELF 64-bit /sample (ELF		6-04-2/sample				1.604.216	0 2023-08-0 REG			nx-dev@nongnu.org
2023-08-0 alpinelinux.org	55062e7a66f7d7a057d8696ec2b6bab8			FALSE			UTF-8 Univ/sample (UTF 8					33.188	148.737	0 2023-08-0 REG	ncopa		copa@alpinelinux.org
	nrsa.pub 35062e7a66f7d7a057d8096ec2b6bab3			FALSE			UTF-8 Unit/sample (UTF 8					33,188	148,737	0 2023-08-0 REG			pine-devel@lists.alpinelinux.org-524d
	ursa.pub 55062e7a66f7d7a057d8696ec2b6bab8			FALSE			UTF-8 Unix/sample (UTF 8					33.188	148.737	0 2023-08-0 REG			pine-devel@lists.alpinelinux.org-5243
	rsa.pub 55062e7a6617d7a057d8696ec2b6bab8			FALSE			UTF-8 Unix/sample (UTF 8					33.188	148,737	0 2023-08-0 REG			bine-devel@lists.alpinelinux.org-5261
2023-08-07 the com.co	5e8512240954499310ab72cc95446be0			TRUE	yang		UTF-8 Unit/sample (UTF 8					33,100	17,280	0 2023-08-0 REG			ao.chaoiun@zte.com.cn
2023-08-07 zte.com.cn	5e8512240954499310ab72rc95446be0			TRUE	yang		UTF-8 Unit/sample (UTF 8					33,188	17,280	0 2023-08-0 REG			ao.chaojun@zte.com.cn
2023-08-0 example.com	50ea12311fae9196ed74100d8325ae1b			FALSE	.txt		news or m/sample (TEXT )					33,188	17,280	0 2023-08-0 REG	VIV		w@example.com
2023-08-0 bitorophet.org	5084d01ara8e7772e625931d28ec1298			TRUE	-04		Python so/sample (PYTHC					33,188	3.922	0 2023-08-0 REG	ieff		ff@bitorophet.org
c2 email-strings	300-40128-40E/1/2E020931028EC1298	+3+310000 3431 /4861 3020	rewo 16:803010	INUE	-97	b4	eAniou and sample That inc	m_megaldfrit201	avoro ( sample	. * 2m/C2/1V	0	30,155	2,922	v 2023-08-0 REG	Jen	e1368300- je	enBorchicking

Figure 69: C2 email addresses (Jarvis)

A B C D E F	G	н	1 J K L	M N AA AB	AC AD	AE	AF	AG J	H N A		AL AM AN	AO AP	AQ AR	AS.	AT AU	AV	AW	AX
@timesta file_info.f file_info.f file_info.f file_info.f file_info.		o.cfile_ini						file_info.sfile_				path query						
2023-08-0: d5ef23a9t 7bfeb6f23 0077c2158 82b07bd3 fcec3a41				IRegularFil 2019-03-01/sample_rVSWc2/N*ef5		33,		0	2023-08-0/REG	rw-rr	github.com		git ef90a9d0-https		hub.com/gevent,			
2023-08-0: d6ef23a9t 7bfeb6f230077c215882b07bd3; fcec3a41			METADAT ASCII text /sample_(PYTHO)	[RegularFil 2019-03-0(/sample_(VSWc2/NVM	e/docki C	33,	188 6,907	0	2023-08-0: REG	196-1-0-	coveralls.io	/github/g-branch	=m ef90a9d0- https	https://con	reralls.io/github/	gevent/geve	ent?branch-	.=master
2023-08-0 d6ef23a9t 7bfeb6f230077c215882b07bd3 fcec3a41	TRUE		METADAT ASCII text /sample_(PYTHON	[RegularFil 2019-03-0/sample_(VSWc2/N ef5	049d0- 0	33,:		0	2023-08-0:REG	DM-1-0-	landscape.io	/github/g-style=	flat ef90a9d0-https	https://lan	dscape.io/github	/gevent/gev	rent/master	r/landscap
2023-08-0: d6ef23a9t 7bfeb6f23 0077c2158 82b07bd3; fcec3a41				_IRegularFil 2019-03-0i/sample_(V5Wc2/NVM		33,		0	2023-08-0 REG	DW-ff	travis-ci.org		-m ef90a9d0- https		vis-ci.org/gevent		rbranch=ma	aster
2023-08-0: d5ef23a9t 7bfeb6f23 0077c2158 82b07bd3: fcec3a415			METADAT ASCII text /sample_(PYTHO)	RegularFil 2019-03-0i/sample_CV5Wc2/NVM	c/docks C	33,:	188 6,907	0	2023-08-0:REG	rw-rr	travis-ci.org	/gevent/gevent	ef90a9d0- https	https://tra	vis-ci.org/gevent	/gevent		
2023-08-0 d5ef23a9t 7bfeb6f23 0077c2158 82b07bd3: fcec3a415	TRUE		METADAT ASCII text /sample_iPYTHON	RegularFil 2019-03-0i/sample_CVSWc2/Nºef5	0u9d0- 0	33,:	188 6,907	. 0	2023-08-0:REG	rw-rr	github.com	/gevent/gevent/	wikef90a9d0-https	https://giti	hub.com/gevent,	gevent/wiki,	/Projects	
2023-08-0 d6ef23a9t 7bfeb6f230077c215882b07bd3 fcec3a415	TRUE		METADAT ASCII text /sample_(PYTHON	IRegularFil 2019-03-0(/sample_(VSWc2/N*ef9	Cu9d0- C	33,3	188 6,907	0	2023-08-0 REG	DW-FF	blog.gevent.org		ef90a9d0-http	http://blog	.gevent.org			
2023-08-01 d5ef23a9t 7bfeb6f23 0077c2158 82b07bd3 fcec3a411	FALSE		METADAT ASCII text /sample_(PYTHON	RegularFil 2019-03-01/sample_(VSWc2/NVM	/docks C	33,	188 6,907	0	2023-08-0: REG	NW-FF	landscape.io	/github/gevent/	gevief90a9d0- https	https://lan	dscape.io/github	/gevent/gev	lent	
2023-08-0: d6ef23a91 7bfeb6f23 0077c2158 82b07bd3: fcec3a41	TRUE		METADAT ASCII text /sample_IPYTHON	IRegularFil 2015-03-01/sample_CVSWc2/N*ef5	04900- 0	33,:	188 6,907	0	2023-08-0:REG	FW-FE	landscape.io	/github/gevent/	gev-ef90a9d0- https	https://lan	dscape.io/githut	/gevent/gev	vent	
2023-08-0: c687ac619 41e903a04 b9ef2affcl df8739ff3x d9bb90c6	TRUE	les.	iso schen XML1.0 di/sample IXML	RegularFil 2019-03-01/sample_CVSWc2/Nº ef5	04960- 0	33,:	188 71,764	0	2023-08-0'REG	DW-1-0-	purl.ocic.org	/dsdl/schematro	n ef90a9d0-http	http://purl	.odc.org/dsdl/sc	hematron		
2023-08-0 c687ac619 41e903a0/ b9ef2affci df8739ff3c d9bb90c6	FALSE	last.	iso scherr XML 1.0 di /sample (XML	RegularFil 2019-03-01/sample (VSWc2/NVM	/docki (	33.	188 71,764	0	2023-08-0'REG	DW-F-F	exsit.org	/dynamic	ef90a9d0-http	http://exsl	t.org/dynamic			
2023-08-0r c687ac619 41e903a0/ b9ef2affct df8739ff3i d9bb90c6	TRUE	lar.	iso schen XML 1.0 di /sample 1XML	RegularFil 2019-03-01/sample <vswc2 n*ef5<="" td=""><td>0a5d0- (</td><td>33.</td><td>188 71,754</td><td>0</td><td>2023-08-0'REG</td><td>nw-r-r-</td><td>exsit.org</td><td>/regular-express</td><td>ion:ef90a9d0-http</td><td>http://exsl</td><td>t.org/regular-exp</td><td>pressions</td><td></td><td></td></vswc2>	0a5d0- (	33.	188 71,754	0	2023-08-0'REG	nw-r-r-	exsit.org	/regular-express	ion:ef90a9d0-http	http://exsl	t.org/regular-exp	pressions		
2023-08-017264ad26k37893fda0ef212bc8f1b5b7984c2d0193b	FALSE		METADAT ASCILLENT /sample (PYTHON	IRegularFil2019-03-0i/sample_CVSWc2/NVM	Visitly (	11.	188 3.335	0	2023-08-0'REG	00-1-0-	travis-ci.org	/chandet/chander	#190a9d0-https	https://tra	vis-ci.org/charde	t/chardet		
2023-08-01 f2b4ad2b8 37893fda0 ef212bc8if 1b5b 7984x c2d0193b				RegularFil 2019-03-0(/sample (VSWc2/NVM		33,	188 3,335	0	2023-08-0'REG	00-1-0-	img.shields.to		svg ef90a9d0-https		shields.io/pypi		18	
2023-08-0/49cb6c241 81d5b059(cb960c022 75644bect 37ab5cf1-		.01		RegularFil 2019-03-0(/sample (VSWc2/NVM		33.		0	2023-08-0'REG	DW-F-F-	pyasn1.sf.net	/license.html	ef90a9d0- http		sn1.sf.net/license		Ĭ	
2023-08-0*4ccc8o485 3dbe5f24i 412e2eo4; 5ab905f99 087d574e		.01		RegularFil 2019-03-0i/sample (VSWc2/N-eff		33.		0	2023-08-0'REG	nv-r-r- t			tm ef90a9d0- http		readthedocs.io/e		et.htmiatti.	-cdef-limit
2023-08-011733a3675 a9a9046bt 239d16db b11edbdd 27c2699b				RegularFil 2019-03-04/sample_CVSWc2/NVM		33.3		0	2023-08-0 REG	DW-1-1-	ucsub.colorado.edu		ef90a9d0-http		/b.colorado.edu/			
2023-08-01698bb7501de36dbd5ab205b7e-4421d326re20e1df6				RegularFil 2019-03-01/sample (VSWc2/NVM		11.			2023-08-0 REG	DW-F-F-	care nist poy		s/fief90a9d0-http		nist.gov/publica			w185.2 or
2023-08-0' 133bb5be cfb2235f1/839a13db/613ab215! 0a35c810				:RegularFil 2019-03-01/sample (VSWc2/NVM		33.		0	2023-08-0'REG	08-1-1-	eli.thegreenplace.		ef90a9d0- http		hegreenplace.ne		taxee at the	same alp
2023-08-074ce98992590a07e3c524a3873aC1c0f967bf 2731d41d				RegularFil 2019-03-01/sample_CVSWc2/NVM		33.		0	2023-08-0'REG	OW-1-F-	python.org		ef90a9d0- http	http://pyt/				
2023-08-0:156a2cdf3 5e399917c cf21f2e0d 8dfcb0c35 cbab1d0f			dv.exe ELF 64-bit /sample (ELF	RegularFil 2019-03-01/sample_CVSWc2/NVM		33.		0	2023-08-0 REG	DW-f-f-	www.openssl.org	/docs/fag.html	ef90a9d0- https		rw.openssl.org/d	locs/face Intend		
2023-08-07 drahfsb/s/9a3282a1z ddg25a5g/8732991br 6964949e				E RegularFil 2019-03-01/sample (VSWc2/NVM		22.		0	2023-08-0'REG	DW-TE	mail.python.org		dev ef90a9d0- http		.python.org/pip			
2023-08-0 0120-9400 945282222 004254546 07529510 09645090 2023-08-0 d53c7ad5t a644c6d3f 5305a94ei 21e81c83a f4f3c7660				:RegularFil 2019-03-01/sample_CV5Wc2/hvm				0	2023-08-0-860	OW-forfor	foo.com	Abiberum Mane-	ef90a9d0- http	http://foo.		annaily icite-c	Nev/2004-01	boenider
2023-08-0 bd969c53c a5c1bdb4: 2c7890d36469f00219 404092cd				:RegularFil2019-03-0//sample_vVSWc2/NVM		33,		0	2023-08-018FG	fW-f-f-	codespeak.net	/lxml/sax.html	ef90a9d0- http		espeak.net/kml	from balant.		
2023-08-0*00969535 a5120054 20190038 469102219 4049200 2023-08-0*b04e02e3*68256c99 5454e14b*15a60849; 3393058c				:RegularFil 2019-03-07/sample_CVSWc2/NVR6 :RegularFil 2019-03-07/sample_CVSWc2/NVR6		33,		0	2023-08-0785G	rw-r-r-	tools.ietf.org	/html/rfc5280	ef90a9d0- https		espeak.net/ixml/ sls.ietf.org/html/			
2023-08-0 D0480283 061C38C97 54548140; 10300849, 3391080 2023-08-0 b06871f28 13b1eab6; aa58f33f2 9ffb91e68 c4351dbe			fontawesi TrueType /sample (TTF	RegularFil 2019-03-01/sample_(VSWc2/NVH)		33.		0	2023-08-0 REG	DW-F-F-	fontawesome.io	/itense	ef90a9d0- https		awesome.io/lice			
2023-08-0 00087122813018408 asor3312 91091898 (4331008 2023-08-0 d1f6c80fc( d8fe5bab; c706c83b6 d72c35a37 b0e07175						33.		U	2023-08-0'REG	DV-folio	www.zte.com.cn	/incense	ef90a9d0- http		w.zte.com.cn	10.24		
2023-08-07 0116c807c1 08765040, c705c8306 072c35a3 / 00607175 2023-08-07 7ae3d4d3-4d8f556et c037c267d c69456962 1a5f70e1		-Yerd		ElRegularFil 2018-05-0:/sample_CVSWc2/Nº ef5				0		DW-f-f-		In the local distance and			w.zte.com.cn Lruu.nl/pub/SGI/	in an		
				RegularFil 2019-03-01/sample_(VSWc2/NVM				0	2023-08-01REG		ftp.cs.ruu.nl	/pub/SGI/FORMS						
2023-08-07 7ae3d4d3-4d8f556et c037c267d c69456962 1a5f70e1			Setup ASCII text /sample_(ASCII	RegularFil 2019-03-04/sample_(VSWc2/NVM/		33,		0	2023-08-0 REG	UM-1-0	www.sleepycat.com				w.sleepycat.com	/update/inde	ex.html	
2023-08-07 7ae3d4d3-4d8f556et c037c267d c69456962 1a5f70e1			Setup ASCII text /sample_(ASCII	RegularFil 2019-03-04/sample_(VSWc2/NVM		33,		0	2023-08-0: REG	rw-rr	www.gzip.org	/zlib	ef90a9d0-http		w.gzip.org/zlib			
2023-08-0: 718285328 9e6c590c6 565960ed; b1093a14( abfbec84			bum.exe ELF 64-bit /sample_(ELF	RegularFil 2019-03-01/sample_CVSWc2/NVM		33,		0	2023-08-0:REG	rw-r-r-	www.zte.com.cn		ef90a9d0- <none></none>	www.zte.c				
2023-08-0:63eab6e3/184fa1a41 7a14c07bi d3553f03c 1ef34352				_(RegularFil 2019-07-21/sample_CVSWc2/NVM		33,		0	2023-08-0:REG	OM-1-L-	www.faqs.org	/rfcs/rfc822.html			w.faqs.org/rfcs/r			
2023-08-0/83ab3674c9312e156/6f2cb18bebe11dff1cdec6fda0		-PV		[RegularFil 2019-03-0(/sample_(VSWc2/NVM		33,		0	2023-08-0 REG	FW-FE	github.com		nik: ef90a9d0- https		hub.com/paramil			4
2023-08-01 a8f2260df 9dx6ccb97 d8f3d996k 4d374509c 51f84ao4			gdbserver ELF 64-bit /sample_tELF	RegularFil 2019-03-01/sample_(VSWc2/NVM		33,		0	2023-08-0 REG	NV-11	www.gnu.org		ugs ef90a9d0- http		w.gnu.org/softw			
2023-08-01 a8f2260df 9do5ccb97 d8f3d9968 4d374509i 51f84ao47			gdbserver ELF 64-bit /sample_tELF	RegularFil 2015-03-01/sample_cVSWc2/N*ef5		33,		0	2023-08-0:REG	fW-f-E-	www.gnu.org		ugs ef90a9d0- http		w.gnu.org/softw			
2023-08-01a8f2260df 9dc6ccb97 d8f3d996t 4d374509i 51f84ao4			gdbserver ELF 64-bit /sample_(ELF	RegularFil 2019-03-01/sample_tusr/bin/gref5		33,2		0	2023-08-0/REG	TWST-RF-X	www.gnu.org		ugs ef90a9d0- http		w.gnu.org/softw		5	
2023-08-0:498fed72Caaf716cd3 b1e57faef e83380c9! ba3e5d82				RegularFil 2019-03-0/sample_(VSWc2/NVM		33,		0	2023-08-0'REG	DM-2-6	github.com		shy ef90a9d0-https		hub.com/pyca/tr	yptography		
2023-08-01 a3cf9a76c. ee44f65di f75259c06 00afa1o4f1 7f2b7968	TRUE	grey-	PucchCon UTF-8 Unb /sample_rUTF_8_1	E RegularFil 2015-03-1:/sample_CVSWc2/Nº ef5	0a9d0- 0	33,	188 4,832	0	2023-08-0'REG	DW-ff	www.zte.com.cn	/5g	ef90a9d0-http		av_zte.com.cn/5g			
2023-08-0: 22da#35%: 64b67ceax da2a7cf53 de0154e5i ab07d775	TRUE	-91	file.py Python so /sample_IPYTHON	RegularFil 2019-03-0i/sample_cVSWc2/N*ef5	04940- 0	33,	188 19,215	0	2023-08-0 REG	rw-rr	www.python.org		/buief90a9d0-http	http://ww	ex.python.org/do	c/current/libs	/built-in-fu	uncs.html
2023-08-0148dbc75c52f8061c3b6621e122(8b9bf4e7;c8589cd7		-91	elliptic_cPython so /sample_IPYTHON	RegularFil 2019-03-0(/sample_CVSWc2/NVM	e/diocks C	33,	188 9,411	0	2023-08-0:REG	DM-10	webpages.charter.	n /curryfans/peter	/do ef90a9d0- http		pages.charter.ne	et/currytans/g	peter/dow	mloads.ht
2023-08-01 c6a00bca8 6f44eb80a 96c53 7f6b cf19a 7baf 504b2e8c	FALSE	-91	url.py Python so /sample_(PYTHON	RegularFil 2019-03-0(/sample_(VSWc2/NVM	v/ssd/v C	33,	188 6,717	0	2023-08-0'REG	DW-E-E	google.com	/mail	ef90a9d0- http	http://goo	gle.com/mail			
2023-08-01ac715f751 1863e035c0a76df6624530d2bc107330e62	FALSE	-91	handler.p Python so /sample_IPYTHON	_tRegularFil 2019-03-0(/sample_tVSWc2/NVM	/ssd/v C	33,	188 14,263	0	2023-08-0:REG	FW-fF	aml.org	/sax/teatures/ex	terief90a9d0-http	http://xml	org/sax/features	/external-pa	arameter-e	ntities
2023-08-0: a4b3db7e 2335d878i 9d3eb602i c9a7d3166 3a348e5f	TRUE	-04	test_robo Python so /sample_rPYTHON	:RegularFil 2019-03-01/sample_rVSWc2/N*ef5	08960- 0	33,:	188 6,980	0	2023-08-0:REG	nw-r-r-	www.robotstxt.org	/wc/norobots.ht	ml ef90a9d0-http	http://ww	w.robotstat.org/e	ec/norobots.	html	
2023-08-0 98601086+61d13a64E0c326e70F03481cbe11d2b46d5	FALSE	-54	pysftp.py Python so /sample_(PYTHO)	RegularFil 2019-03-01/sample_CVSWc2/NVM	/docks 0	33,	188 36,938	0	2023-08-0 REG	rw-r p	aramiko. paramiko-docs.rea	d /en/latest highlig	tht: ef90a9d0- http	http://para	miko-docs.readt	hedocs.org/e	en/latest/a	pi/sftp.ht
2023-08-010c2a0d2c6 2633c0e2a fo45fe00e eb79dd08 88dbe763	FALSE	.91	test utilit Python so /sample (PYTHON	RegularFil 2019-03-0(/sample_CVSWc2/NVM	/docks 0	33,	188 56,079	0	2023-08-0'REG	DW-F-E	example.com	/ni	ef90a9d0-http	http://exa	mple.com/ni	1.00		
2023-08-0 0c2a0d2c6 2633c0e2a fo45fe00e eb79dd08 88dbe765	FALSE	-01		RegularFil 2019-03-01/sample_cvSWc2/NVM		33.	188 56.079	0	2023-08-0:REG	DW-F-F-	example.com	/foo	ef90a9d0- http	http://exa	mple.com/too			
2023-08-070c2a0d2c6 2633c0e2a fo45fe00e eb 79dd08 88dbe763	TRUE	.OV		:RegularFil 2019-03-04/sample (VSWc2/N1ef5		33.	188 56.079	0	2023-08-0'REG	00-1-1-	example.com	/100	ef90a9d0-http	http://exa	mple.com/foo			
2023-08-010c2a0d2c62633c0e2zfc45fe00eeb79dd0888dbe763				RegularFil 2019-03-0(/sample_(VSWc2/NVM		33.3		0	2023-08-0 REG	DW-FE	example.com	/spam	ef90a9d0- http		mole.com/spam			
c) c2 url-strings +																		

Figure 70: C2 URL Report (Jarvis)

2 > Т	EST V					Do	ownload ~
Overview	Bill of Materials Findings Scans	Files					
	Risk 100 / 100 0 10 35 Findings Detected 10K Software Components 1,679	65 100	Details Operating Systems À Linux Kernel 4.4.39, Linux K VXWorks Unknown ▲ A Architectures - Products Depending On This Ar August 2023 Created € charles.begian@ngc.com August 30, 2023	Ipine Lini			nel 4.4.97
	Finding Exploit Intelligence	<i>l</i> ₹ Count	Remediation Guidance 🕠				
	No Known Exploits	8,288 findings	Guidance	4₹	As	sociated I	Findings
	Proof of Concept Exploit	©1,833 findings	Address high risk component Linux Kernel 3.10.55	6	25	94	1,275
	4 Weaponized	0 86 findings	Address high risk component Linux Kernel 4.4.39	2	21	82	1,020
	Reported in the Wild	0 27 findings	Address high risk component Linux Kernel 4.4.97	0	17	79	977
	Exploited By Threat Actors	0 17 findings	Address high risk component tcpdump 4.9.0	3	84	26	3

# Sample C2 Finite State Platform Scan Report Excerpts

Figure 71: C2 Scan Overview (Finite State Platform)

C2 >	TEST ~ ) iew Bill of Materials <b>Findings</b> Scans	Files					Downloa	ad ~ Upload
Findi	ngs by Severity 10K findings Low (7285) • Medium (2412) • High (451) • Critical	I (59) • Unkn	own (O)		Finding Exploit Intellige       Category       No Known Exploits       Proof of Concept Exploit       Y       Weaponized       Image: Separate In the Wild       Exploited By Threat	ploit		IF Count           8,288 findings           ○ 1,833 findings           ○ 27 findings           ○ 17 findings
161	Filter Q. Search findings							
	Title	Severity	≒ Risk	Status	CVE	CWE	Found By	Date
	CVE-2017-18017 - Linux Kernel:4.4.39	Critical	<b>9.7</b> /10		CVE-2017-18017	CWE-416	Finite State Monitoring	Aug 31, 2023
	CVE-2017-18017 - Linux Kernel:3.10.55	Critical	9.7/10		CVE-2017-18017	CWE-416	Finite State Monitoring	Aug 31, 2023
	CVE-2019-12815 - ProFTPD:1.2.5 🔞	Critical	<b>9.7</b> /10		CVE-2019-12815	CWE-755	Finite State Monitoring	Aug 31, 2023
	CVE-2016-2108 - OpenSSL:0.9.8za	Critical	9.7/10		CVE-2016-2108	CWE-119	Finite State Monitoring	Aug 31, 2023
	CVE-2016-2108 - OpenSSL:1.0.1f	Critical	<b>9.7</b> /10		CVE-2016-2108	CWE-119	Finite State Monitoring	Aug 31, 2023
	CVE-2017-7895 - Linux Kernel:3.10.55	Critical	9.6/10		CVE-2017-7895	CWE-119	Finite State Monitoring	Aug 31, 2023

D	E
category	subcategory
CREDENTIALS	PASSWD_USER_ACCOUNTS
CRYPTO_MATERIAL	PEM_CERTIFICATE_KEY
CRYPTO_MATERIAL	EXPIRED_CERTIFICATE
CRYPTO_MATERIAL	PEM_CERTIFICATE_EXPIRED
SAST_ANALYSIS	USE_AFTER_FREE
SAST_ANALYSIS	DOUBLE_FREE
CONFIG_ISSUES	SSH_PERMIT_ROOT
SAST_ANALYSIS	INCORRECT_RANDOM_USAGE
SAST_ANALYSIS	UNCHECKED_RETURN_VALUE
SAST_ANALYSIS	EXPRESSION_ALWAYS_TRUE
SAST_ANALYSIS	INHERENTLY_DANGEROUS_FUNCTION
SAST_ANALYSIS	IMPROPER_LENGTH_HANDLING
SAST_ANALYSIS	INCORRECT_BEHAVIOR_ORDER
SAST_ANALYSIS	VERY_HIGH_CODE_COMPLEXITY
SAST_ANALYSIS	HIGH_CODE_COMPLEXITY
CREDENTIALS	SHADOW_HARD_CODED_PASSWORDS
CREDENTIALS	PASSWD_HARD_CODED_PASSWORDS
CREDENTIALS	BLANK_ROOT_PASSWORDS
CRYPTO_MATERIAL	SSH_PRIVATE_KEY
CRYPTO_MATERIAL	SSL_PRIVATE_KEY
CRYPTO_MATERIAL	SELF_SIGNED_CERT
SAST_ANALYSIS	VXWORKS_EXE_NO_PASSWORD
SAST_ANALYSIS	STACK_BUFFER_OVERFLOW
CVE	KNOWN_VULNERABILITIES
> C2_TEST.	findings +

А	В	C D	G	Н	I
vulnIdFromTool		cvssV3Sco cvssVectorString	affectedComponents		maxExploitMaturit
CVE-2017-3730	7.4	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	4	рос
CVE-2016-8610	7.3	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2016-6305	7.2	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2016-7054	7.4	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	2	рос
CVE-2016-6304	7.2	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2017-3730	7.4	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	4	рос
CVE-2016-8610	7.3	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2016-6305	7.2	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2016-7054	7.4	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	2	рос
CVE-2016-6304	7.2	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0	1	рос
CVE-2021-43527	7.3	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NSS:3.12.4	1	рос
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2n	1	poc
CVE-2018-0500	8.3	9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.55.1	1	poc
CVE-2019-3822	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.55.1	1	poc
CVE-2019-5436	7.3	7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	cURL:7.55.1	1	poc
CVE-2016-8610	7.3	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.0.2g	1	poc
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2g	1	poc
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2j		poc
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1		poc
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1		poc
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2k		poc
CVE-2016-8610	7.3	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.0.2e		poc
CVE-2022-1292	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2e		poc
CVE-2016-6304	7.2	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.0.2e		poc
CVE-2016-6304	7.2	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.0.1f		poc
CVE-2014-0224	7.4	7.4 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N			weaponized
CVE-2014-0160	7.5	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	OpenSSL:1.0.1f		weaponized
CVE-2015-0292	7.2		OpenSSL:1.0.1f		poc
CVE-2019-3822	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.52.1		poc
CVE-2019-5436	7.3	7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	cURL:7.52.1		poc
CVE-2019-3822	9.5	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.57.0		poc
CVE-2019-5436	7.3	7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	cURL:7.57.0		poc
CVE-2019-0400	8.3	9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.57.0		poc
CVE-2018-20843	7.4	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	expat:2.1.0		poc
CVE-2018-20845	7.3	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	expat:2.1.0		poc
CVE-2022-25236	8.7	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	expat:2.1.0		poc
CVE-2022-25236	8.7	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	expat:2.1.1		poc
CVE-2022-20230	7.4	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	expat:2.1.1		poc
CVE-2018-20843	7.4	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	expat:2.1.1		poc
CVE-2022-23313	7.5	8.1 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:3.10.55		
CVE-2013-0574	7.4	7.5 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:3.10.55		poc
		7.5 CVSS:3.1/AV:N/AC:L/PR:N/01:N/S:0/C:N/1:N/A:H			poc
CVE-2015-4004	7.5	7.5 CVCC-2.1 (AVIN (A CH / DDIN (HIN) (CH / CH / HALAH	Linux Kernel:3.10.55		poc
CVE-2014-3687	7	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:3.10.55		poc
CVE-2019-11478	7.5	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:3.10.55		poc
CVE-2019-11477	7.5	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:3.10.55		poc
CVE-2016-5195	7.7	7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:3.10.55		weaponized
CVE-2020-14305	7.3	8.1 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H			. poc
CVE-2019-11479	7.5	7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.4.39		. poc
CVE-2019-11478	7.5	7.5 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.4.39	1	poc

### Figure 73: C2 Findings Categories (Finite State Platform)

Figure 74: C2 CVE Exploitability (Finite State Platform)

# **APPENDIX E: CST SCAN REPORT EXCERPTS FOR SAMPLE C3**

Black Duck Binary Analysis Search a	and jump to group 순 Upload • ⑦ • 온 charles.begian •
Analysis settings File content	
General	
Name	sample_C3.zip 🗹
Description	No description given 🗹
Version	No version given 🗹
Uploaded	2023-08-10 02:43 (5 days ago) by charles.begian
Last scanned	2023-08-10 03:59 (5 days ago)
BDBA engine version used for scanning	20230608
BDBA frontend version used for calculation	20230615 LATEST
Protect from data retention	
Notify on new vulnerabilities	
File properties	
File	全, Replace
File available	No
SHA1	3015b74e30d22a49c4badfada99430152959f77a
Size	4.29 GB (original) / 16.31 GB (scanned)
Analysis © Remove	
Application type	Linux kernel
Duration	an hour
Throughput ①	73.54 MB/s
BDSA database version ①	2023-08-14T11:59:50 STALE
NVD database version ③	2023-08-14T06:15:00 STALE
Component database version $ \odot $	2023-08-14T04:04:31
Native fingerprint version	2023-05-31T10:04:47
Dotnet fingerprint version	2023-05-31T04:12:23.653096
Cocoapods fingerprint version	2023-06-07T07:52:47.754010
Golang fingerprint version	2023-06-08T07:16:22.448950
Python fingerprint version	2023-06-12T01:47:49.220082
Low risk tolerance mode	No (0)
Include historical vulnerabilities	Yes ©

# Sample C3 Black Duck Scan Report Excerpts

Figure 75: C3 Scan Overview (Black Duck)

# sample\_C3.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY

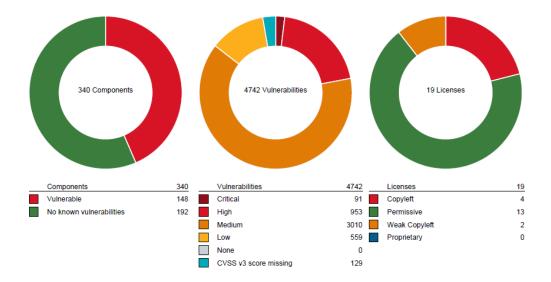


Figure 76: C3 Scan found 4742 Vulnerabilities (Black Duck)

Original filename SHA1 checksum	3015b74e30d22a49c4badfada99430152959f77a	
Original file size	30150746300222449040a0fa0a99430152959177a 4292.88 MB	
Original ne size	4232.00 MD	
Infoleak		
Asymmetric keys:	1351	
is result is a product of an automatic	analysis and may contain errors or omissions.	Page 589/590
AWS keys:	0	
AWS keys: Custom pattern matches:	0 0	
-	-	
Custom pattern matches:	0	
Custom pattern matches: Emails:	0 15350	
Custom pattern matches: Emails: HTTP authentication:	0 15350 0	
Custom pattern matches: Emails: HTTP authentication: Image metadata:	0 15350 0 0	
Custom pattern matches: Emails: HTTP authentication: Image metadata: IP addresses:	0 15350 0 0 14970	
Custom pattern matches: Emails: HTTP authentication: Image metadata: IP addresses: JSON web tokens:	0 15350 0 0 14970 0	
Custom pattern matches: Emails: HTTP authentication: Image metadata: IP addresses: JSON web tokens: MAC addresses: OAuth tokens: Passwords:	0 15350 0 0 14970 0 184 0 397	
Custom pattern matches: Emails: HTTP authentication: Image metadata: IP addresses: JSON web tokens: MAC addresses: OAuth tokens: Passwords: Shell history:	0 15350 0 0 14970 0 184 0 397 10	
Custom pattern matches: Emails: HTTP authentication: Image metadata: IP addresses: JSON web tokens: MAC addresses: OAuth tokens: Passwords: Shell history: URLs:	0 15350 0 0 14970 0 184 0 397	
Custom pattern matches: Emails: HTTP authentication: Image metadata: IP addresses: JSON web tokens: MAC addresses: OAuth tokens: Passwords: Shell history:	0 15350 0 0 14970 0 184 0 397 10	

Figure 77: C3 Information leaks (Black Duck)

Aleorithm	Dite Council	Driveta	Encrypted	Contrast	User	Everience	Continue	xAttributes	Cila .				-		-	-				-		-	-	-		-								
Aguinin	0 PEM	TRUE		BEGIN ENCRYPTED PRIVATE KEY	usei	copiles	Cerunitat			C3.zip', 'V	nu da lan	Malarist	e ldede	reldariar	leadertenh	habbe	-lehansel	-	17-5310	Ris 201año	500-811-s7	6-70/6	A REAL	1410-0	415-5915	ed later	Unerine	Dibibboo	lles ner					
	0 PEM	TRUE		······BEGIN ENCRYPTED PRIVATE KEY																										9b55f43e4d				
201	1024 PEM																										, uspilea	79-2PU2-1	14.181, 308	9000143640	100503083	08600/1403	62342210	00334041
DSA		TRUE		BEGIN DSA PRIVATE KEY						_C3.zip', 'V																								
	0 PEM	TRUE	TRUE	BEGIN ENCRYPTED PRIVATE KEY						C3.zip', 'V																								
	0 PEM	TRUE	TRUE	BEGIN ENCRYPTED PRIVATE KEY					['sample	C3.zip', 'V	SW612/NV	Me/ssd/1	version	/VER/V2.2	1.01.0089	199-2P02-	14_20210	825191325	5.ospf", "V	2.21.01.00	1899-2202	14_2021	08251913	25.ospf-	128-37667	i62.lama	', 'ospf@8	99-2902-1	14.tar', '568	9b55f43e4d	a08ed90a9	ba8cb7f4d!	62342276	rdc334b417
RSA	2048 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY					['sample	C3.zip', 'V	SWd2/NV	Me/docke	r/overia	sy2/434eet	f0049aefd	ic81bd42c	d8de2220	91e55196	i6446e1a	25cee3d0a	76528664	591/diff	etc/ssh/s	sh_host	rsa_key]									
RSA	2048 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY					['sample	C3.zip', 'V	swd2/NV	Me/ssd/1	version	/VER/V2.2	1.01.0089	199-2P02-	14_20210	25191325	5.webmn	ť, V2.21.0	11.00899-2	P02-14	02108251	91325.v	vebmnt-12	8-361587	09.lama', '	webmnt(	@899-2P02	14.tar', '3a9	414869916	5830e9204e	89c28e258	k5320b8a6
DSA	1024 PEM	TRUE	FALSE	BEGIN DSA PRIVATE KEY					l'sample	C3.zip', 'V	swd2/w	Me/ssd/1	version	/VER/10SN	NV2.21.07	17.088170	0824 5g.	A9622A52	16Cpu', '11	0SWV2.21	.07.088170	0824 5	A9622A9	26Cpu-4	109630-23	357403.g	z', 'uboot-	fw.ing', '	uboot-fw.i	mgi, 'etc/ssi	h/ssh hos	t dsa kev/l		
RSA	2048 PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY																		-				_		-		14.tar', '3a5				c5300b8a6
RSA	2048 PEM	TRUE	FAISE	BEGIN RSA PRIVATE KEY						C3.zip', 'V																								
RSA	2048 PEM	TRUE		BEGIN RSA PRIVATE KEY						C3.zip', 'V																								
RSA	1024 PFM	TRUE	FALSE	BEGIN RSA PRIVATE KEY						(3.zip', 'V																	Version	Nib/Nibrov	sng.soʻl					
RSA	2048 PEM	TRUE	FAISE	BEGIN RSA PRIVATE KEY																									nfig/beego	kev]				
RSA	2048 PFM	TRUE		BEGIN RSA PRIVATE KEY																									nfig/server					
RSA	1024 PEM	TRUE		BEGIN RSA PRIVATE KEY																										9655f43e4d	-00-400-0	hadab 1644		-
RSA	2048 PEM	TRUC		······BEGIN RSA PRIVATE KEY																														10(224041)
		INUE																												mg', 'etc/ssi				
RSA	4096 DER	TRUE		'BEGIN PRIVATE KEY																			20210825	191325.	VswdCpu-	6821-94	38040.gz',	V2.21.01	.00899-290	2-14_202100	25191325	VswdCpu-:	6821-943	8040"]
RSA	4096 DER	TRUE	FALSE	BEGIN PRIVATE KEY					['sample	C3.zip', 'V	SWd2/Tu	ffDrive/Pa	rtition3/	BIN/cpu_c	cur.swv, \	'qpu_cur	SWV-1683	1-9438040	0.gz', 'cpu	i_cur.siw-	16821-943	8040"]												
ECDSA	256 PEM	TRUE	FALSE	BEGIN EC PRIVATE KEY					['sample	C3.zip', 'V.	SWd2/NV	Me/ssd/1,	version	/VER/105V	NV2.21.07	17.088170	10824_5g.	A9622AS2	16Cpu', '1	0SWV2.21	.07.088170	0824_5	A9622AS	26Cpu-4	109630-23	357403.g	z', 'uboot-	fw.ing', '	'uboot-fw.i	mg', 'etc/ssl	h/ssh_hos	t_ecdsa_ke	1	

### Figure 78: C3 Asymmetric keys (Black Duck)

A	8 C	D	E	Ŧ	G	н	1	1	ĸ	1	М	N	0	P	Q	R 5
Algorithm Bits	Format	Private	Encrypted Conte		User	Expires	Certificat	x Attributes	File							
RSA	1024 PEM	FALSE	FALSEB	EGIN PUBLIC KEY					['sample_C3	Lzip', 'VSV	ud2/NVM	e/docker/	overlay2/c	Tee7d6e638	F83d54a160	d6536471a0d933
RSA	4096 PEM	FALSE	FALSEB	EGIN PUBLIC KEY		2042-01-12718:59:32	TRUE	("countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 63")	['sample_C3	szip', 'VSV	ud2/NVM	e/ssd/1/w	ersion/VER	/V2.21.01.00	699-2P02-1	4_202108251913
RSA	2048 PEM	FALSE	FALSEB	IEGIN PUBLIC KEY		2025-05-12723:59:00	TRUE	("countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimore CyberTrust Root")	['sample_C3	B.zip', 'VSV	udz/NVM	e/ssd/1/w	ersion/VER	/V2.21.01.00	899-2P02-1	4_202106251913
RSA	2048 PEM	FALSE	FALSE	EGIN PUBLIC KEY		2037-12-01723:59:59	TRUE	("countryName": "US", "organizationName": "VeriSign, Inc.", "organizationalUnitName": "(c) 2008 VeriSign, Inc For authorized use only", "commonName": "VeriSign Univ	['sample_C3	Lzip', 'VSV	ud2/NVM	e/ssd/1/v	ersion/VER	/V2.21.01.00	899-2P02-1	4_20210825191
RSA	2048 PEM	FALSE	FALSE -B	EGIN PUBLIC KEY		2029-12-31723:59:59	TRUE	["countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COMODO CA Limited", "commonName": "COMOD	['sample_C3	azip', 'VSV	ud2/NVM	e/ssd/1/w	ersion/VER	/V2.21.01.00	899-2P02-1	4_20210825191
RSA	4096 PEM	FALSE	FALSEB	EGIN PUBLIC KEY		2038-07-31712:29:50	TRUE	["countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "A82743287", "organizationName": "AC Camerfin	['sample_C3	Lzip', 'VSV	ud2/NVM	e/ssd/1/v	ersion/VER	V2.21.01.00	899-2P02-1	4_20210825191
RSA	2048 PEM	FALSE	FALSE	EGIN PUBLIC KEY		2029-12-31717-28:07	TRUE	("countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TirustCor Systems S. de R.L.", "organizationalUnitName": "	['sample_C3	Lzip', 'VSV	ud2/NVM	e/ssd/1/v	ersion/VER	V2.21.01.00	1899-2P02-1	4_20210825191
RSA	4096 PEM	FALSE	FALSEB	EGIN PUBLIC KEY		2042-02-05109:27:35	TRUE	["countryName": "RO", "organizationName": "CERTSIGN SA", "organizationalUnitName": "certSIGN ROOT CA G2"]	['sample_C3	aip', 'VSV	ud2/NVM	e/ssd/1/v	ersion/VER	V2.21.01.00	899-2P02-1	4_20210825191
RSA	4096 PEM	FALSE	FALSE 'B	EGIN PUBLIC KEY		2042-01-12718:59:32	TRUE	["countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 63"]	['sample C3	szip', 'VSV	ud2/NVM	e/ssd/1/w	ersion/VER	V2.21.01.00	899-2P02-1	4 20210825191
RSA	2048 PEM	FALSE	FALSEB	EGIN PUBLIC KEY		2025-05-12723:59:00	TRUE	["countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimore CyberTrust Root")	['sample_C3	Lzip', 'VSV	udz/NVM	e/ssd/1/w	ersion/VER	/V2.21.01.00	1899-2P02-1	4_20210825191
RSA	2048 PEM	FALSE	FALSE	EGIN PUBLIC KEY		2037-12-01723:59:59	TRUE	("countryName": "US", "organizationName": "VeriSign, inc.", "organizationalUnitName": "(c) 2008 VeriSign, inc For authorized use only", "commonName": "VeriSign Univ	('sample_C3	Lzip', 'VSV	ud2/NVM	e/ssd/1/v	ersion/VER	V2.21.01.00	899-2P02-1	4 20210825191
RSA	2048 PEM	FALSE	FALSEB	EGIN PUBLIC KEY		2029-12-31723:59:59	TRUE	["countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COMODO CA Limited", "commonName": "COMODO	['sample_C3	aip', 'VSV	udz/NVM	e/ssd/1/o	ersion/VER	V2.21.01.00	899-2P02-1	4 20210825191
RSA	4096 PEM	FALSE	FALSE	EGIN PUBLIC KEY		2038-07-31712-29:50	TRUE	["countryName": "FU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "A82743287", "organizationName": "AC Camerfin	['sample_C3	Lzip', 'VSV	ud2/NVM	e/ssd/1/o	ersion/VER	V2.21.01.00	1899-2P02-1	4_20210825191
RSA	2048 PEM	FALSE	FALSE	EGIN PUBLIC KEY		2029-12-31717:28:07	TRUE	["countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Systems S. de R.L.", "organizationalUnitName":	['sample_C3	Laip', 'VSV	ud2/NVM	e/ssd/1/w	ersion/VER	V2.21.01.00	1899-2P02-1	4_20210625191
RSA	4096 PEM	FALSE	FALSE '	EGIN PUBLIC KEY		2042-02-05109:27:35	TRUE	["countryName": "RO", "organizationName": "CERTSIGN SA", "organizationalUnitName": "certSIGN ROOT CA G2"]	['sample_C3	zip', 'VSV	ud2/NVM	e/ssd/1/v	ersion/VER	V2.21.01.00	899-2P02-1	4 20210825191
RSA	1024 PEM	FALSE	FALSEB	EGIN PUBLIC KEY					['sample_C3	s.zip', 'VSV	udz/NVM	e/registry	/docker/do	cker/registr	y/v2/blobs	/sha256/40/400
RSA	2048 PEM	FALSE	FALSEB	EGIN PUBLIC KEY		2037-02-22717:02:16	TRUE	["organizationName": "www.zte.com.on", "organizationalUnitName": "27E", "commonName": "2te.com.on WebMNT"]	['sample_C3	Lzip', 'VSV	udz/NVM	e/ssd/1/ld	g/itran_log	/webmnt/w	vebmnt-201	180501-000816-
RSA	2048 PEM	FALSE	FALSE -B	EGIN PUBLIC KEY		2037-02-12708:20:25	TRUE	("organizationName": "www.zte.com.cn", "organizationalUnitName": "ZTE", "commonName": "Zte.com.cn WebMNT")	['sample_C3	zip', 'VSV	ud2/NVM	e/ssd/1/lo	g/itran_log	/webmnt/s	vebmnt-203	180501-000816-
RSA	1024 PEM	FALSE	FALSE -B	EGIN PUBLIC KEY					['sample_C3	Lzip', 'VSV	ud2/NVM	e/ssd/1/w	ersion/VER	/v2.21.01.00	1899-2P02-1	4_20210825191
	A196 DEM	Failer	Thier 1 D	EGIN PUBLIC KEY		2042-01-12718-59:32	TDUE	["countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 63"]	Pramole (1)	inin' 'USU	an Inna	Institute	Ideebarlin	renelansiste	Sablah	/sha256/7b/7b

### Figure 79: C3 Symmetric keys (Black Duck)

1 Email	File	Domain
2 umac-64@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/045db4ac22ab5b77df2287a32a72570e56005e33b105bb63c7804884e70bc7f7/diff/etc/ssh/ssh_config']	openssh.com
hmac-md5-96-etm@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/bin/ssh']	openssh.com
zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/bin/ssh']	openssh.com
eow@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/bin/ssh']	openssh.com
hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/49e6f9604d3c68c9768e6e38e77dd4acd088f661812aee28dc1f2a77819c151c/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
0 ftp@example.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/4c91d67/f800ea56f5e75cb3606194032d2e148992f855e011ec8b7fae0b13e50/diff/urllc-uds-snr]	example.com
1 zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlav2/4d3d0ce77ba9dfa9165cb307f59c683765c10b99def4c5c708053ab1f8e17fbf/diff/home/weblmt/load/RebexTinySftpServer.zip', 'Rebex	TinySflopenssh.com
hmac-md5-96-etm@openssh.com	['sample_C3.zjp', VSWd2/NVMe/docker/overlay2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/bin/ssh']	openssh.com
3 zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/bin/ssh']	openssh.com
4 eow@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/bin/ssh']	openssh.com
5 hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlav2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
6 zlib@openssh.com	[sample_C3.zip], VSWd2/NVMe/docker/overlav2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
7 hmac-md5-96-etm@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
zlib@openssh.com	[sample_C3.zip], VSWd2/NVMe/docker/overlav2/50862bc48351d99727277a80a8a444d94bdecb9a5a932bf16e4c3e32b2f581b6/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
ftp@example.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/51d8446f1e5afb7c4703e8c0cddb7caae5a37919e281faa6ba8d7ff640e34bce/diff/tcfslib/libcurl.so.4.6.0']	example.com
hmac-md5-96-etm@openssh.com	[sample_C3.zip], VSWd2/NVMe/docker/overlav2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/bin/ssh]	openssh.com
1 zlib@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/bin/ssh]	openssh.com
2 eow@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/bin/ssh']	openssh.com
hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/bin/ssh-keyscan']	openssh.com
zlib@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/bin/ssh-keyscan']	openssh.com
5 hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/libexec/openssh/ssh-keysign']	openssh.com
5 zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5206fa40cbc92759d2411d06652d056a5596e291090cf7242b122c2b5f3aeb3e/diff/usr/libexec/openssh/ssh-keysign']	openssh.com
7 ftp@example.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/6594d5d5f9290c35bf2fa018a544ea3860110d008a5281d7007eab7baaf1c9c8/diff/tcfslib/libcurl.so.4.6.0']	example.com
ftp@example.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/67e9a8ed7ef905bb2d87edb3217e05f6063b2c4a9ce14b69fc105bc0ac17f631/diff/ids']	example.com
ftp@example.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/6d6ed7ab593eb2e737ecea3b973275074d6d8d8c1edfc0f58ca90e55c5758e98/diff/tcfslib/libcurl.so.4.4.0']	example.com
ftp@example.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/737cbae5c1f52097df5a37f954daf1f1dfb85b0848d018038dd3e37f63d73010/diff/hucm']	example.com
1 hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/bin/ssh']	openssh.com
2 zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/bin/ssh']	openssh.com
eow@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/bin/ssh']	openssh.com
4 hmac-md5-96-etm@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
5 zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
6 hmac-md5-96-etm@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
7 zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75123a48a3f478c0ca497874c6e1e2fe08a2476a1991cf4b520f1ada2513924f/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
ftp@example.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/77d9e00c1fa152693f5957bd4c60b948e19500faa01778f95a2850a65e724710/diff/Irrm_Iff]	example.com
ftp@example.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/7853de3b6a930a3f79b32ad27b40c17522fb5442e2c4e3458b4a1f1d30ddee60/diff/mim']	example.com
me@example.org	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/8002cee813d9672356159bfc32c5308e06de3ccf1c4526b6a45a61946ffa7c6d/diff/nfamp/bin/nfamp.exe']	example.org
1 hmac-md5-96-etm@openssh.com	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/81f9b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/bin/ssh']	openssh.com
zlib@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/81f9b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/bin/ssh']	openssh.com
eow@openssh.com	[sample_C3.zip', VSWd2/NVMe/docker/overlay2/81f9b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/bin/ssh1]	openssh.com
4 hmac-md5-96-etm@openssh.com	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/81f9b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/bin/ssh-keyscan']	openssh.com
5 zlib@openssh.com	['sample: C3.zip', 'VSWd2/NVMe/docker/overlay2/81f9b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/bin/ssh-keyscan']	openssh.com
6 hmac-md5-96-etm@openssh.com	[sample_C3.zip], VSWd2/NVMe/docker/overlay2/81f9b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/libexec/openssh/ssh-keysign]	openssh.com
7 zlib@openssh.com	[sample_C3.zip', VSWd2/NVMe/docker/overlay2/819b97a4e906f3727460f7d04ae7eb808554d69372de59fb2bfa7834cb0d4cd/diff/usr/libexec/openssh/ssh-keysign']	openssh.com
C3 infoleak-emails		1.1

Figure 80: C3 Infoleak email addresses (Black Duck)

129

			U	
31         22.54.12.1         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/00d1es1952c9808bh1e43111913H7282cd0574e10333ce614s6efdx/conftg.v2.joon           31         23.254.55.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/00d1es1952c9808bh1e43111913H7282cd0574e10333ce614s6efdx/conftg.v2.joon           31         25.254.116         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/04d02a1e13b270808bh2e355548020801e2442233779sedee7d55d72/conftg.v2.joon           31         25.455.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/04d02a1e13b2708012643223779sedee7d55d72/conftg.v2.joon           32         25.45.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/04d02a1e13b27a05b20643208012e44223779sedee7d55d72/creoix.conf1           32         25.45.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/0222737b1abs60fd44b83745131491544a312ab264f27498e7dee185d71[scoix.conf1           32         25.45.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/0222727b1abs60fd44b83745131491544a312ab264f27498e7dee185/config.v2.joon1           32         25.45.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/0222727b1abs60fd44b83745131491544a312ab264f27498e7dee186/scoix.conf1           32         25.45.16         FASE:         Sample C. 3.17; VSWd2/NVM/obcker/container/0222727b1abs60fd44b83745131491544a312ab264f27498e7dee186/scoix.conf1           32         25.45.16         FASE: <t< td=""><td>1</td><td>IP</td><td>IPv6</td><td>File</td></t<>	1	IP	IPv6	File
1         27.324.122         FASE         Sample C.3.17; VSWd2/NVM/docker/container/0014c19152c9808bd1e34111911782cda0574e310333ce614a5e1de4/conftq.v2.jpon1           6         132.345.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/01402aa1eb14b7abc0b8355bf480028bb1e2442237b79easee7d55d72/conftg.v2.jpon1           7         172.545.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/10402aa1eb14b7abc0b8355bf480028bb1e24442237b79easee7d55d72/conftg.v2.jpon1           8         8.4.4         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/10402aa1eb14b7abc0b8355bf480028bb1e24442237b79easee7d55d72/conftg.v2.jpon1           8         8.4.4         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/10402aa1eb14b7abc0b8355bf480028bb1e2442237b79easee7d55d72/reotv.conf1           173.2545.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/10222757b1bas6d144b8a74fs1174e514c8312abbf37d9ae7dee18/scnftg.v2.jpon1           173.2545.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/0222757b1bas6d144b8a74fs1174e5134c8312abbf37d9ae7dee18/scnftg.v2.jpon1           173.2545.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/0222757b1bas6d144b8a74fs1174e5132c82bbc1a545c7449426964(conftg.v2.jpon1           173.2545.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/0538d77c442332260469e2202398a21h8951cc6a845c74942d6966(conftg.v2.jpon1           173.2545.16         FASE         Fismple C.3.17; VSWd2/NVM/docker/container/056313276642032398a21h8951cc	2	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
9         17.2349.516         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/01402a1etbit/bb7bc2603520H4002030b1e24442327779eaisee7df5577/config.v2.jsom1           7         17.354.55.10         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/01402a1etbit/bb7bc26053250H4002030b1e24442237779eaisee7df55777/resolv.conf]           17.20.1         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/01402a1etbit/bb7bc26053250H4002020b1e244422337779eaisee7df554777/resolv.conf]           18.2.4.1.16         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/01402a1etbit/bb7bbc26053250H4002020b1e244422337779eaisee7df554777/resolv.conf]           17.2.544.5.10         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/01402a1etbit/bb7bbc26053250H4002020b1e244422337779eaisee7df554777/resolv.conf]           17.2.544.5.10         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/0127227873blaa60fd44bd5a7451374615448312bb4174059ae7dee189/rosolv.conf]           17.2.544.5.10         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/0127227873blaa60fd44bd5a7451374615448312bb4174059ae7dee189/rosolv.conf]           17.2.554.1.16         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/013380727ac4433322600d9e20223355624b632bb520bc305457c43293d0566/ros0ling.v2_joon1]           17.2.554.1.16         FAISE         ['sample_C3::p', 'SW22/WWWe/docker/containers/053380727ac4433322600d9e20223356624b632b52bb20bc305457c43293d0566/ros0ling.v2_joon1]            17.2.554.1.16         FAISE         ['sample_C3::p',	з	192.254.128.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
9         19.254.116         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/04/02aaleb1b4/bb2/bb225b44002200b1e24442237/breakee7d5557/.host5]           9         8.8.8         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/04/02aaleb1b4/bb2/bb225b525b46002200b1e24442237/breakee7d5557/.host5]           9         8.8.8         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/04/02aaleb1b4/bb7bb22b63525b46002200b1e24442237/breakee7d5557/.resolv.comf]           11         12.254.116         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0422aaleb1b4b7bb22b63525b46002200b1e24442237/breakee7d5557/.resolv.comf]           11         12.254.116         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0222b73b1aa601444b6a74314a514463142b647a708e70dee197/.oncol.comf]           12.254.116         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0222b73b1aa601444b6a743146514468112b6467a708e70dee197/.oncol.comf]           13.254.511         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0222b73b1aa601444b6a743146514468112b647a708e70dee197/.oncol.comf]           13.254.511         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0222b73b1aa601444b6a7431465144b6a74308e70dee197/.oncol.comf]           13.254.512         FALSE         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0222b6314b6202b2034565744923d0560/.oncf]         ['sample_C.st.p', 'VSW2/VWWe/docker/containers/0222b6314b6202b2033565746922b6305563466749234056050/.oncf]         ['sazzsss.st.p'ss.st.p'ss.st.p'ss.st.p's	4	173.254.128.2	FALSE	['sample C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
7         72 <th72< th="">         72         <th72< th="">         72         <th72< th="">         72<td>5</td><td>173.254.95.16</td><td>FALSE</td><td>['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']</td></th72<></th72<></th72<>	5	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
Interpret/1000000000000000000000000000000000000	6	192.254.1.16	FALSE	['sample C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/config.v2.json']
9         8.8.8         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b635256144802028b1e244423237b7es6ee7df55d72/resolv.conf]           182.254.1.16         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/01222673b1aa80f044db8a7bf317446194ca3312bb6f7a09ae7dee169/config.v2.jonf]           182.254.1.16         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/0222673b1aa80f044db8a7bf317446194ca3312bb6f7a09ae7dee169/config.v2.jonf]           182.354.51.6         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/0222673b1aa80f044db8a7bf317446194ca3312bb6f7a09ae7dee169/resolv.conf]           18.8.4         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/0222673b1aa80f044db8a7bf3174d51343312bb6f7a09ae7dee169/resolv.conf]           19.2254.1.16         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/0222673b1aa80f044db8a7bf3174d51343322b60f64520a23938c716952bc0a348573492d5066/ronfig.v2.jonf]           19.2254.1.26         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/05338727cad433226d069e20a23938c716952bc0a348757492d5066/ronfig.v2.jonf]           19.2254.1.28         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/0566132256144e0120e0933ebc118b73cee881a307876sbc2b2584c0(onfig.v2.jonf]           19.2254.1.28         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/0566132256614e0210e0933ebc118b73cee881a307876sbc2b2584c0(onfig.v2.jonf)           19.2254.1.28         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/05673230402227de24101312ae85d218b973cee8881a307876s	7	173.254.95.16	FALSE	[sample C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/config.v2.json']
10         8.4.4         FALSE         Tsample (3.1µ), VSW2/NVMe/docker/containers/(072287581bas60f44db837456174691048312bb46fa7099ac7dbe169/config.v2.jon?)           11         192.254.116         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/(072267361bas60f44db837456174691948312bb46fa7099ac7dbe169/config.v2.jon?)           12         1273.254.93.6         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/(072267361bas60f44db83745131746194ca8312bb46fa7099ac7dbe169/config.v2.jon?)           13         127.0.1         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/(022267361bas60f44db83745131746194ca8312bb46fa7099ac7dbe169/ros0).conf]           13         22.54.1.16         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/(023267361bas60f44db83745131746194ca8312bb46fa7099ac7dbe169/ros0).conf]           13         22.54.1.16         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/03380727cad43322600d9e520a2398ac71b692bbc30a549c734229dd506a/config.v2.jon?]           13         25.54.1.16         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/05380727cad4332260d9e520a2398ac71b692bbc30a549c734292dd506a/config.v2.jon?]           13         25.54.1.16         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/056533275614e0210e093abc211b873ce8881a07876sbc2525540/config.v2.jon?]           13         25.254.1.16         FALSE         [sample (3.1µ), VSW2/NVMe/docker/containers/056533275614e0210e093abc211b873ce8881a078776sbc52552540/config.v2.jon?]           13 </td <td>8</td> <td>127.0.0.1</td> <td>FALSE</td> <td>['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/hosts']</td>	8	127.0.0.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/hosts']
11         12         12.25.41.16         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/config.v2.jon1           12         127.0.0.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)           18         8.8.4         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)           19         22.541.16         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)         Containers/027267361baa60fd4b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)           19         22.541.16         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05380477ca4423322d60dee220a23936a2fab692bbc30a549c7a9429d566a/config.v2.jon1           19         12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05380477ca423322d60dee220a23936a2fab692bbc30a549c7a9429d566a/config.v2.jon1           19         12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05661322C5614e0210e933eb2ef18b9f3cee8681a30789765cba25583dca764292405664/config.v2.jon1           12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05661322C5614e0210e933eb2ef18b9f3cee8681a30789765cba25583dca764929405664/config.v2.jon1           12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/contain	9	8.8.8.8	FALSE	[sample C3.zip], 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/resolv.conf']
11         12         12.25.41.16         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/config.v2.jon1           12         127.0.0.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)           18         8.8.4         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)           19         22.541.16         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/0272267361baa60fd44b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)         Containers/027267361baa60fd4b8a745fa31746154ca831a2bb46fa7a09ae70dee169/rost)           19         22.541.16         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05380477ca4423322d60dee220a23936a2fab692bbc30a549c7a9429d566a/config.v2.jon1           19         12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05380477ca423322d60dee220a23936a2fab692bbc30a549c7a9429d566a/config.v2.jon1           19         12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05661322C5614e0210e933eb2ef18b9f3cee8681a30789765cba25583dca764292405664/config.v2.jon1           12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/containers/05661322C5614e0210e933eb2ef18b9f3cee8681a30789765cba25583dca764929405664/config.v2.jon1           12.254.12.1         FALSE         [Sample_C3.1p], 'USWd2/WVMe/docker/contain	10	8.8.4.4		
12       173.254.95.16       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/0272267361baa60fd4db8a745fa3174a6134c831a2bb46fa7a697ade169/nost]         13       127.0.0.1       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/027227361baa60fd4db8a745fa3174a6134c831a2bb46fa7a697ade26fa97es0x.com]         15       8.8.4       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/027227361baa60fd4db8a745fa3174a6134c831a2bb46fa7a697ade26f360s/config.v2.json]         16       132.254.11.6       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/03380727cad423322d60dbe220a2398a2fab692bbc30a549c7a9429dd506a/config.v2.json]         17       132.254.12.1       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/0538047crad423322d60dbe220a2398a2fab692bbc30a549c7a9429dd506a/config.v2.json]         17       132.354.12.2       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/0538047crad423322d60dbe220a2398a2fab692bbc30a549c7a9429dd506a/config.v2.json]         173.254.91.16       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/055661322c56614e0210e0938b2ef18b9f3csee8681a307897865a2ba258e3dfconfig.v2.json]         173.254.91.16       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/05561322c56614e0210e0938b2ef18b9f3csee8681a307897865a2ba258e3d/config.v2.json]         173.254.91.16       FALSE       ['sample_C3.ip', 'SWd2/NVMe/docker/containers/0552310a0227de241013f32ae85dd2b998bab40b12231980rd48a333d/config.v2.json]         173.254.95.16       FALSE       ['sample_C3.ip', 'S	11	192,254,1,16		
13         127.0.0.1         FALSE         ['sample_G.2:p', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db837451a31746194c831a2b46fa7a09ae70dee169/resolv.conf]'           14         8.8.8.3         FALSE         ['sample_G.2:p', 'VSWd2/NVMe/docker/containers/027267361baa60fd44db837451a31746194c8331a2b46fa7a09ae70dee169/resolv.conf]'           15         8.8.4.4         FALSE         ['sample_G.2:p', 'VSWd2/NVMe/docker/containers/0333677cad423322d6009e6220a2336a2fb652bbc3084597a429d5056a/conftex2.jsonf]           17         1252.541.16         FALSE         ['sample_G.2:p', 'VSWd2/NVMe/docker/containers/0333677cad423322d6009e6220a2336a2fb652bbc3084597a429d506a/conftex2.jsonf]           17         252.451.81         FALSE         ['sample_G.2:p', 'VSWd2/NVMe/docker/containers/05661322c56614e0110e0338e12afbbf92bc308459c7a9429d506a/conftex2.jsonf]           172.254.128.1         FALSE         ['sample_G.3:p', 'VSWd2/NVMe/docker/containers/05661322c56614e0110e0338e12afbbf93c3ee861a30787656ac2a5bc34/conftex2.jsonf]           173.254.128.1         FALSE         ['sample_G.3:p', 'VSWd2/NVMe/docker/containers/05661322c56614e0110e0338e12afbbf93c3ee861a30787656ac2a5bc34/conftex2.jsonf]           173.254.128.1         FALSE         ['sample_G.3:p', 'VSWd2/NVMe/docker/containers/0667352130e02a7/de2110873c2e86d1a90978765ac2a5bc34/conftex2.jsonf]           173.254.128.1         FALSE         ['sample_G.3:p', 'VSWd2/NVMe/docker/containers/0667352130e02a7/de2110873c2e86d120959a3b460b1223199e7d4e33a34/contors]           173.254.126.5         FALSE				
14         B.8.8.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/027267361baa60fd44db83745fa31746194c8312bb6fa7a09ae70dee189/resolv.conf]           15         B.8.4.4         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/0338077cad423322d6009e6220a23936a7b652bbc30a549c73423d5056a/config.v2_json]           17         192.254.12.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/0338077cad423322d6009e6220a23936a7b652bbc30a549c73423d5056a/config.v2_json]           17         192.254.12.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/05338077cad423322d6009e6220a23936a7b652bbc30a549c7a9423d5056a/config.v2_json]           17         192.254.12.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/05661322c56614e0110e0338bc2f1ab9f3cae861a30737865ac2ba558c3/config.v2_json]           18         12.254.12.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/05661322c56614e0110e0338bc2f1ab9f3cae861a30737865ac2ba558c3/config.v2_json]           19         12.254.12.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/0667352130e02a27de241013f3cae86dd2b99e3ab640b1223199e07de33a33/config.v2_json]           19         12.254.12.8         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/0667352130e02a27de241013f3cae85dd2b99e3ab640b1223199e07de433a33/config.v2_json]           19         12.254.12.6         FALSE         ["sample_C3.zip", VSWd2/NVMe/docker/containers/0675352130e02a27de241013f3cae85dd2b99e3ab640b1223199e07				
15         8.8.4         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/0272267361baa60fd4dbba745fa174a6194c831a2bbd6fa7a09ae70dee169/resolv.conf]           16         192.254.11.6         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/0338d72rad423322600596220a23936a2fab692bbc30a549c7a492405066/config.v2.json1]           173.254.128.2         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/0538d72rad423322600596220a23936a2fab692bbc30a549c7a492405066/config.v2.json1]           173.254.128.2         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/0538d72rad423322600596220a23936a2fab692bbc30a549c7a492405066/config.v2.json1]           173.254.128.1         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/05661322c566140210e0933eb2ef18b9f3c3ee8681a3078765acb235540/config.v2.json1]           173.254.95.16         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/05661322c566140210e0933eb2ef18b9f3c3ee8681a3078765acb235540/config.v2.json1]           173.254.95.16         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/056732130e02a7rde4101372ae85dd2b99e3ab6db122139e074e3333d/config.v2.json1]           173.254.95.16         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/067352130e02a7rde4101372ae85dd2b99e3ab6db122139e074e3333d/config.v2.json1]           173.254.95.16         FALSE         ['sample_G3.rb', VSWd2/NVWe/docker/containers/067352130e02a7rde4101372ae85dd2b99e3ab6db122139e074e3333d/config.v2.json1]           173.254.95.16         FALSE         ['sample_G3.rb', VSWd2/NVW				
16         192.254.1.1.6         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/05338d72rcad423322d60d95202a3396a2fab692bbc30a549c7a429d3050a/config.v2.jon']           17         192.254.128.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/05338d72rcad423322d60d95202a3396a2fab692bbc30a549c7a492d3050a/config.v2.jon']           18         17.254.156.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/0538d72rcad423322d60d95202a3396a2fab692bbc30a549c7a492d3050a/config.v2.jon']           19         12.254.16         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/05661322c56614e0210e0933ebc2f18b9f3cae8681a30789786sacba5584d/config.v2.jon']           19         12.254.126.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/05661322c56614e0210e0933ebc2f18b9f3cae8681a30789786sacba5584d/config.v2.jon']           17         17.254.35.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/056735130e02a27de241013f32ae85dd2b998ab64b1223198e07d483383d/config.v2.jon']           17         17.3254.35.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/066735130e02a27de241013f32ae85dd2b998ab64b1223198e07d483383d/config.v2.jon']           173.254.35.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/0667352130e02a27de241013f32ae85dd2b998ab64b1223198e07d483383d/config.v2.jon']           183.254.35.1         FALSE         ['sample_G3.tp', VSWd2/NVWe/docker/containers/0667352130e02a27de241013f32ae85dd2b998ab64b1223198e07d483383d/config.v2.jon']				
17       192.254.128.1       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/05388d72rcad423322d60d9e6220a3936a2fab692bcba08467ra9429dd506a/config.v2.json']         18       173.254.128.2       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/05388d72rcad423322d60d9e6220a3936a2fab692bcb008450ra9429dd506a/config.v2.json']         197.12.954.128.1       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/05661322c5614e0210e093aeb2f18b9f3cee8681a07897865acb255e3d/config.v2.json']         192.254.128.1       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/05661322c5614e0210e0933eb2f18b9f3cee8681a07897865acb255e3d/config.v2.json']         173.254.95.16       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/05661322c5614e0210e0933eb2f18b9f3cee8681a07897865acb255e3d/config.v2.json']         173.254.95.16       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/0567352130e02a7de241013f32ae65d2b99e3ab6401223193e07d4e33a3d/config.v2.json']         173.254.95.16       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/067352130e02a7de241013f32ae65d2b99e3ab6401223193e07d4e33a3d/config.v2.json']         173.254.95.16       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/067352130e02a7de241013f32ae65d2b99e3ab6401223193e07d4e33a3d/config.v2.json']         173.254.95.16       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/containers/067352130e02a7de241013f32ae65d2b99e3ab6401223193e07d4e33a3d/resolv.conf]       192.254.116         183.4       FALSE       ['sample_C3.1p', VSWd2/NVMe/docker/container				
18         173.254.128.2         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/05338d727cad423322d60d9e6220a23938a2fab692bbc30a549c7a9429d506a/config.v2.json']           19         173.254.55.16         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/05661322c5661420210e0933eb2fab973c3ee8681a907897865acb258e3d/config.v2.json']           19         192.254.128.1         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/05661322c5661420210e0933eb2fab973c3ee8681a907897865acb255e3d/config.v2.json']           19         172.254.128.2         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/05661322c5661420210e933eb2fab973c3ee8681a907897865acb255e3d/config.v2.json']           19         172.254.128.1         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/0567352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/config.v2.json']           19         172.254.55.16         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/0567352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/config.v2.json']           19         12.254.126         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/057352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/config.v2.json']           19         12.254.126         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/06755213b71d10b771e590915c3062300007f1a495574151e04e8e2aba20/config.v2.json']           19         12.254.126         FALSE         ['sample_G3.tip', 'VSWd2/NVMe/docker/containers/075752b71				
19         173.254.95.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/05338d727cad423322d60d9e6220a23936a2fab692bbc30a549c7a9429d506a/config v2.json']           19         1272.254.1.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/05661322256614e0210e0933eb2e1ab973c3ee8681a307897865acb2a55e3d/config v2.json']           19         1272.554.128.1         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/05666132256614e0210e0933eb2e1ab973c3ee8681a307897865acb2a55e3d/config v2.json']           19         1272.554.128.2         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/05661322130e02a27de241013f32ae85dd2b99e3ab640b122319807d4e33a3d/config v2.json']           19         1272.554.95.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b122319807d4e33a3d/config v2.json']           10         1272.0.1         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b122319807d4e33a3d/cnofig v2.json']           10         1272.541.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/067352130e02a27de241013f32ae85dd2b99e3ab640b122319807d4e33a3d/resolv.conf]           19         1272.541.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/067352130e02a27de241013f32ae85dd2b99e3ab640b122319807d4e33a3d/resolv.conf]           19         1272.541.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/067352130e02a27de24101				
20         192.254.1.16         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2e18b9f3c3ee8681a307897865acb2a55e3d/config v2.json']           21         12.254.128.1         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2e18b9f3c3ee8681a307897865acb2a55e3d/config v2.json']           21         17.254.95.16         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2e18b9f3c3ee8681a307897865acb2a55e3d/config v2.json']           21         17.254.95.16         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85d2b99e3ab64b1223199207de33a3d/config v2.json']           21         17.254.95.16         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85d2b99e3ab64b1223199207de433a3d/resolv.conf]           21         88.4.4         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85d2b99e3ab64b1223199207de433a3d/resolv.conf]           28         88.4.4         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/0679527bb71d10b7571e590915c062300020781a495574151e048e2aba20/config v2.json']           29         254.128.1         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/0679527bb71d10b7571e590915c062300020781a495574151e048e2aba20/config v2.json']           20         2254.126         FALSE         ['sample_C3.rip', VSWd2/NVMe/docker/containers/0679527bb71d10b7571e590915c062300020781a4955741				
11         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/05661322c5614e0210e0933eb2ef18b9f3c3ee8681a3078785cab2a55e3d/config.v2.json]           12         I73.254.128.2         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/05661322c5614e0210e0933eb2ef18b9f3c3ee8681a3078785cab2a55e3d/config.v2.json]           137.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de33a33d/config.v2.json'           127.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de33a33d/config.v2.json'           127.0.0.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/resolv.conf]           128.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/resolv.conf]           129.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/067352130e02a7de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/resolv.conf]           192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/067352130e02a7de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/resolv.conf]           192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0675521b071d1f0b757Le590915c30623002078f1a495574151e04e8e2aba20/config.v2.json']           172.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVM				
22         173.254.128.2         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/05661322c56614e0210e0933eb2e118b9f3c3ee8681a307897865acb2355e3d/config.v2.json']           23         173.254.95.16         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/056752130e02a27de241013f32ae85dd2999a3b640b1223193e07de433a33d/config.v2.json']           24         192.254.116         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2999a3b640b1223193e07de433a33d/config.v2.json']           25         173.254.95.16         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2999a3b640b1223193e07de433a33d/resolv.conf]]           26         8.8.8         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/067552130e02a27de241013f32ae85dd2999a3b640b1223193e07de433a3d/resolv.conf]]           28         8.8.4         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/0675527bb71d1f0b7571E590915c3062300078f1a495574151e04e8ee2aba20/config.v2.json']           29         125.254.128.1         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/0675527bb71d1f0b7571E590915c30623000078f1a495574151e04e8ee2aba20/config.v2.json']           2173.254.95.16         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/0915f1a95c34b03768785c097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']           2173.254.95.16         FALSE         ['sample_G3.zip', VSWd2/NVMe/docker/containers/0915f1a95c34b03768785c097ec315a83d2d1b5170cc43f35fde256eb0f650/				
23       173.254.95.16       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/config.v2.json']         24       192.254.1.16       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/config.v2.json']         25       173.254.95.16       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/nosts']         2127.0.0.1       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/resolv.conf]         218.8.8       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/067552130e02a27de241013f32ae85dd2b99e3ab640b1223193e07de433a33d/resolv.conf]         219.2.54.1.16       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/0675527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']         217.3.54.128.2       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/0675527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']         217.3.54.128.2       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/091bf1a95c3db03708785c907ec315a832d1b5170cc43f35fde256eb0f50/config.v2.json']         217.3.54.9.516       FALSE       ['sample_C3.zip', VSWd2/NVMe/docker/containers/091bf1a95c3db03768785c907ec315a832d1b5170cc43f35fde256eb0f50/config.v2.json']         217.3.54.9.516       FALSE       ['sample_C3.zip', VSWd2/NV				
24         192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139ae07d4e33a33d/config.v2.json'           25         773.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139ae07d4e33a33d/config.v2.json'           26         28.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139ae07d4e33a33d/config.v2.json'           27         8.8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/067352130e02a27de241013f32ae85dd2b99e3ab640b1223139e07d4e33a33d/config.v2.json'           28         8.4.4         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0673527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json'           29         22.54.128.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json'           21         73.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json'           21         73.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce8db0376878c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json'           21         73.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce8db0				
25       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139a07d4e33a33d/nost5]         26       1270.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139a07d4e33a33d/nost5]         27       8.8.8.8       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139a07d4e33a33d/nost5]         28       8.8.4       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/067352130e02a27de241013f32ae85dd2b99e3ab640b1223139a07d4e33a33d/nost5]         29       192.254.128.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0673527bb71d1f0b7571e590915:30623002078f1a495574151e04e8ee2aba20/config.v2.json']         21       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915:30623002078f1a495574151e04e8ee2aba20/config.v2.json']         21       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915:30623002078f1a495574151e04e8ee2aba20/config.v2.json']         21       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785:097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']         21       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/081bf395ec8db03768785:097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']				
26         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/resolv.comf]           27         8.8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/resolv.comf]           28         8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/resolv.comf]           29         254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b757le590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           2173.254.128.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b757le590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           2173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b757le590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           2173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']           2173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.comf']           2173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d989856d9312bb7c322ec34e2b955fc26af1fa8b508d0da892a6H1b03/config.v2.json']           2				
27         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139e07d4e33a33d/resolv.conf]           28         8.8.4         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223139e07d4e33a33d/resolv.conf]           29         192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b757Le590915:30623002078f1a495574151e0488ee2aba20/config.v2.json']           31         173.254.92.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b757Le590915:30623002078f1a495574151e0488ee2aba20/config.v2.json']           31         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/097952b7b71d1f0b757Le590915:30623002078f1a495574151e0488ee2aba20/config.v2.json']           31         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091552b671d1f0b757Le590915:30623002078f1a495574151e0488ee2aba20/config.v2.json']           31         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0915f1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           31         173.254.91.6         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08154955c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           32         173.254.91.6         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec34e2b				
28         8.8.4.4         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d483a33d/resolv.conf]           29         192.254.1.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json]           30         173.254.128.1         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json]           31         173.254.95.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json]           32         173.254.95.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec3158a3d2d1b5170cc43f35fde256eb0f650/config.v2.json]           31         173.254.95.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec3158a3d2d1b5170cc43f35fde256eb0f650/config.v2.json]           32         127.0.0.1         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec3158a3d2d1b5170cc43f35fde256eb0f650/cronfig.v2.json]           38         8.8.4         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec3158a3d2d1b5170cc43f35fde256eb0f650/cronfig.v2.json]           39         173.254.95.16         FALSE         ['sample_C3.zip', VSWd2/NVMe/docker/containers/0816989586d312bb7cc				
29         192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           30         192.254.128.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           31         173.254.128.2         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           31         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           32         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db0376878c9097ec315a83d2d1b5170cc43735fde256eb0f560/cnsolv.config.v2.json']           34         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db0376878c9097ec315a83d2d1b5170cc43735fde256eb0f560/resolv.conf']           35         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db0376878c9097ec315a83d2d1b5170cc43735fde256eb0f50/resolv.conf']           36         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d698958d9312bb7c322ec34e2b955fc26af1fa8b5608d0a892a641b03/config.v2.json']           378.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d698958d9312bb7c322ec34a				
30         192.254.128.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           31         173.254.128.2         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           32         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           31         192.254.116         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a955c48b03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f550/config.v2.json']           31         192.254.116         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f550/resolv.conf]           32         127.0.0.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f550/resolv.conf]           38         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           39         127.0.0.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           30         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d93				
11       173.254.128.2       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb7ld1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']         12       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95c8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']         13       122.54.1.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95c8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']         14       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95c8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']         15       127.0.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95c8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']         18       8.8.8       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95c8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']         19       127.0.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']         19       127.0.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']         19       127.0.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf'] <td>_</td> <td></td> <td></td> <td></td>	_			
32         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']           33         192.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']           34         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']           35         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           36         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           37         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0846989586d9312bb7c322ec3a4e2b55fc26af1fa8b5608d0da892a641b03/config.v2.json']           38         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b55fc26af1fa8b5608d0da892a641b03/config.v2.json']           39         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b55fc26af1fa8b5608d0da892a641b03/config.v2.json']           40         28.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b				
33         192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce3db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']           34         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce3db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']           35         127.0.0.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce3db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           36         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce3db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           37         8.8.4.4         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ce3db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           39         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           30         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           31         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           32         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4				
34         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/hosts']           35         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/hosts']           36         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf]           37         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf]           38         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json]           39         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/hosts']           40         18.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/hosts']           41         8.8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf]           42         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6811526f76b97427ea3b206d68d9d9d5f/config.v2.json]				
35         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           36         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           37         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           38         8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           39         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           40         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/rosolv.conf']           41         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/rosolv.conf']           42         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7c322ec34e2b955fc26af1fa8b5608d0da892a641b03/rosolv.conf']           43         29.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d698936d5312bb7cc322ec34e2b955fc26af1fa8b5608d0d8892a641b03/rosolv				
36         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           37         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/081bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']           38         8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           39         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           40         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/costf']           42         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           42         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           43         192.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b9560c38f37939e01abd51dcf6811526f76b97427ea3b206d68d949d5f/config.v2.json']           44         TA2556.5.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f379399e01abd51dcf6811526f76b97427ea3b2				
37       8.8.4.4       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95cc8db03768785c9097cc315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf]         38       192.254.1.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json]         39       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json]         40       127.0.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/cost]         42       8.8.8       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf]         42       8.8.4       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf]         43       192.254.1.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d9698586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf]         44       173.254.95.16       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/08d90e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json]         45       127.0.0.1       FALSE       ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json] <td< td=""><td></td><td></td><td></td><td></td></td<>				
38         192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           39         173.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           40         127.0.0.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/nosts']           41         8.8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf]           42         8.8.4.4         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf]           43         192.254.1.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           44         7a.254.95.16         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         127.0.0.1         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/rosf]           46         8.8.8         FALSE         ['sample_G3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b974				
39         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']           40         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/hosts']           41         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           42         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           43         192.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a9b0e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           44         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a9b0e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a9b0e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a9b0e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/rost]           47         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a9b0e06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d				
40         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/hosts']           41         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           42         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           43         192.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           44         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           46         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f379399e01abd51dcf6e811526f76b97427ea3b20				
41         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           42         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7c322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           43         19.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           44         7.554.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           46         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']				
42         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']           43         192.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b9742rea3b206d68d949d5f/config.v2.json']           44         173.554.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b9742rea3b206d68d949d5f/config.v2.json']           54         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b9742rea3b206d68d949d5f/rosts']           6         8.8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b9742rea3b206d68d949d5f/rosts']           7         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b9742rea3b206d68d949d5f/resolv.conf']				
43         192.254.1.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           44         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/roots']           46         8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/roots']           47         8.8.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']				
44         173.254.95.16         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']           45         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/hosts']           46         8.8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']				
45         127.0.0.1         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/nosts']           46         8.8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']				
46         8.8.8.8         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']           47         8.8.4.4         FALSE         ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']				
47 8.8.4.4 FALSE ['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']				
< > C3 infoleak-ips +	47	8.8.4.4	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/resolv.conf']
		$\langle \rangle$	C3 infoleak-ips	+

## Figure 81: Infoleak IP addresses (Black Duck)

A	В	C C
Address	Vendor	File
00:11:22:33:44:55	CIMSYS Inc	['sample_c3.zip', VSWd2/NVMe/docker/overlay2/l434eef0049aefc81bd42cd8de222091e551966446e1a25cee3d0a7b528d64591/diff/etc/network/interfaces']
00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_c3.zip', VSWd2/NVMe/docker/overlay2/6e445d276e1fb93acbaba9e3b141aa5d01250ab83ea5bce700f7c983f74c3cc/diff/vm_deploy.json']
00:11:22:33:44:55	CIMSYS Inc	["sample_c3.zip], 'V5Wd2/NVMe/docker/overlay2/75080e74e03ac9855559x8d4cf185b2580dcf5ab37bc33187acb309f2a2cd0cef/diff/etc/network/interfaces]
00:11:22:33:44:55	CIMSYS Inc	['sample_c3.zip', VSWd2/NVMe/docker/overlay2/831d1aa8a958adf2652f85b2b24e49396f0c4cce755f67927342f33086ae346b/diff/etc.nommu/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	["sample_c3.zip', VSWd2/NVMe/docker/overlay2/831d1aa8a958adf2652f85b2b24e49396f0otcce755f67927342f33086ae346b/diff/etc/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/f5b980a914e117a5fba7b5678566b872fdb1ac65f07eead284573b82e377804d/diff/etc.nommu/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	["sample_c3.zip', VSWd2/NVMe/docker/overlay2/f55980a94e117a5fba7b5678566b872fdb1ac65f07eead284573b82e377804d/diff/etc/network/interfaces']
00:D0:D0:BA:EB:CA	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BSP/BoardInit.log.bak.1', 'BoardInit.log.bak']
00:D0:D0:CA:42:FB	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BSP/BoardInit.log.bak.10, 'BoardInit.log.bak']
00:D0:D0:5A:D6:6F	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/Boardinit.log.bak.11', 'Boardinit.log.bak']
00:D0:D0:EA:AD:85	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BSP/BoardInit.log.bak.12', 'BoardInit.log.bak']
00:D0:D0:9A:19:FE	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/Boardinit.log.bak.13', 'Boardinit.log.bak']
00:D0:D0:5A:80:DD	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BS9/Boardinit.log.bak.14', Boardinit.log.bak']
00:D0:D0:BA:89:BA	ZHONGXING TELECOM LTD.	[sample_C3.zip', VSWd2/NVMe/logs/BSP/Boardinit.log.bak.15', Boardinit.log.bak']
00:D0:D0:4A:2D:F0	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BSP/Boardinit.log.bak.16', Boardinit.log.bak']
00:D0:D0:4A:CA:3F	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BSP/Boardinit.log.bak.2', 'Boardinit.log.bak.4']
00:D0:D0:DA:07:7C	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/Boardinit.log.bak.3', 'Boardinit.log.bak']
00:D0:D0:3A:08:FD	ZHONGXING TELECOM LTD.	['sample_C3.zip', VSWd2/NVMe/logs/BSP/Boardinit.log.bak.4', 'Boardinit.log.bak.4'
00:D0:D0:7A:12:D7	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'vSWd2/NVMe/logs/BSP/Boardinit.log.bak.5', 'Boardinit.log.bak']
00:D0:D0:AA:62:DF	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVWe/logs/BSP/Boardinit.log.bak.6', 'Boardinit.log.bak']
00:D0:D0:FA:16:D4	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'vSWd2/NVMe/logs/BSP/Boardinit.log.bak.7', 'Boardinit.log.bak']
00:D0:D0:AA:78:E3	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/Boardinit.log.bak.8', 'Boardinit.log.bak']
00:D0:D0:4A:AE:D5	ZHONGXING TELECOM LTD.	[sample_C3.zib', VSWd2/NVWe/logs/BS9/Boardinit.log.bak/9', Boardinit.log.bak/
00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log']
00:00:00:00:22:00	Officially Xerox	[sample_C3.zib', VSWd2/NVWe/logs/BS5//Bs0Moni.log.bak.1', 'Bs0Moni.log.bak']
00:00:00:00:22:00	Officially Xerox	['sample C3.zip', 'VSWd2/NVMe/Jog/B/S/BpMoni.Jog.bak2,' BspMoni.Jog.bak']
00:00:00:00:22:00	Officially Xerox	[sample Gatip' VSWd2/WWW/bgd5/S58/S00/nl.log.bak3," StoMonil.og.bak1
00:00:00:00:22:00	Officially Xerox	['sample_G3.zip', VSWd2/NVMe/jog/859/8pMoni.log.bak4,' spMoni.log.bak'
00:00:00:00:22:00	Officially Xerox	[sample (3.t); //SWd2/NWM/log/SS/SSM0ni.log.bak/, //SSM0ni.log.bak/
00:00:00:00:22:00	Officially Xerox	Lasting_Coupy, Constructional Instruction Construction Co
00:00:00:00:22:00	Officially Xerox	[sample (3.t); VSW2(VMWM/log(sS/SS)SM0/nl.log.bak7, VSW2(VMW/log(sSS)SM0/nl.log.bak7)
00:d0:d0:ff:ff:fe	ZHONGXING TELECOM LTD.	[ambre_Colory, Vord/New/New/New/New/New/New/New/New/New/New
00:00:00:00:22:00	Officially Xerox	Landpa_calp/_varmer/ngr/varmer/ngr
00:00:00:00:22:00	Officially Xerox	[ambm_colum_s, column_log(column_log(column_log), superiording, column_log(column_log)] ['sample (S.i)' ('SWG/UNM/log(s)/SB/UNDerken3.0g')
00:00:00:00:22:00	Officially Xerox	[ample_cash/ vstra/strue/ng/legs/legs/legs/legs/egs/
00:11:22:33:44:55	CIMSYS Inc	[3m1pm] y = 2 may y = 2 may y = max = 2 may y = max = 2 may y = 2 may
00:11:22:33:44:55	CIMSYS Inc	[mmpe_cate], / SW02/WW1/Pegistry/docker/docker/egistry/syndown/wate
00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	[ample_5.a]/ Vstru/Tvtwr/registry/dockr/igotxif/activ/fig/sity/2/bio/s/site2/6/a/6848-e96531860519224220772c8b6495160031968235196000557ac1000001]
00:00:00:FF:FF:FF	Officially Xerox	[ampine_cs.np, vs.wu/rww/rejstri/yoocker/oocker/rejstri/y/z/tioos/smaco/ea/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
00:00:00:00:FF:FF:FF	CIMSYS Inc	[sample_C3.mp; VsWd2/WWh(registry)ooker(roboxer(registry)/2/lobo/shazbr/n)/nocked/31b3/7bdoe8127b6/ab1exbbezebesi/e/shabalaoboba1ab2/1000/1482, "RUSNd/pjenvj_Socketmooule.oo] ['sample_C3.mp; VsWd2/WWh(registry)ooker(roboxer(registry)/2/lobo/shazbr/n)/ab1exbezebesi/e/shabalaoboba1ab2/1000/1482, "RUSNd/pjenvj_Socketmooule.oo]
		[ampin1.s.p, vswu2/vvw/regstry/acocker/acstry/acocker/agstry/2/bios/sta26/a/a/ar060essi1/acockess
00:19:84:07:23:00 00:21:85:28:31:50	ESTIC Corporation MICRO-STAR INT'L CO., LTD.	[sample_cs.np, vswdu/www.registry/docker/jestry/v/looks/nacsequal/abs/statics/
00:21:85:28:31:50 00:d0:d0:0a:01:01		[sample_51.pt; VsWd2/WWheresttyr/docker/socker/registry/2/block/hat2bre/ctdo15728884c4x359e318950428e46ba359e3189504273bab4374521/dta14; "NicsNog/singli.tit.it.", Singli dl/NDSNG_0AM_TXT.dtr] ['sample_51.pt; VsWd2/WWheresttyr/docker/socker/socker/block/bb3564fadeba2888e4x3539e31895028e46bba5273bab43752207bab4375221/dta14; "NicsNog/singli.tit.it.", Singli dl/NDSNG_0AM_TXT.dtr]
	ZHONGXING TELECOM LTD.	
44:33:4C:06:06:ee		,tl['sample_C3.zip', 'SVMdZ/NVMe/ssc/1/svm/VER/10374.VswdBoct', 'ramfisk.hin', 'boot.out']
00:11:22:00:11:22	CIMSYS Inc	['sample_C3.zip', 'SYMd2/NVIMe/ssd/L/symn/VER/L037A.VswdBoot', 'ramdisk.bin', 'boot.out']
00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	['sample_C3.zip', 'v5Wd2/NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', 'boot.out']

Figure 82: C3 Infoleak MAC addresses (Black Duck)

A	В	C	D	E	F
Password	User	Algorithm		Hashed	
	zte		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/045db4ac22ab5b77df2287a32a72570e56005e33b105bb63c7804884e70bc7f7/dff/etc/passwd-']
	root		FALSE		['sample_c3.zip', 'VSWd2/NVMe/docker/overlay2/045db4ac22ab5b77df2287a32a72570e56005e33b105bb63c7804884e70bc7f7/diff/etc/passwd-']
	zte		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0aS2404b6282027d1ba51af16e17514d946e53260a69c0b8/diff/etc/passwd']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0a52404b6282027d1ba51af16e17514d946e53260a69c0b8/diff/etc/passwd']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0a52404b6282027d1ba51af16e17514d946e53260a69c0b8/diff/etc/passwd-']
	zte		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/etc/passwd']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/etc/passwd']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/etc/passwd-']
	zte		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/2cdd6c8060c93d7109b4324b022ff4b546394332dc687e50cfcbff2829b58276/diff/etc/passwd-']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/2cdd6c8060c93d7109b4324b022ff4b546394332dc687e50cfcbff2829b58276/diff/etc/passwd-']
	zte		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/3a332f830ae0c3c8f628cd3b11d2d21f9acb7fdbe09b16477d1abcf4d9a65289/diff/etc/passwd-']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/3a332f830ae0c3c8f628cd3b11d2d21f9acb7fdbe09b16477d1abcf4d9a65289/diff/etc/passwd-]
	zte		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlay2/54afd749f3900a3da1d908d3062993369af13693f07d4d2e7a33bb37e8e54787/diff/etc/passwd-']
	root		FALSE	FALSE	['sample_C3.zip', VSWd2/NVMe/docker/overlav2/54afd749f3900a3da1d908d3062993369af13693f07d4d2e7a33bb37e8e54787/diff/etc/passwd-']
r8tVEoIOxiI0FBrtOjf3HbJp1QA68twJMj9bnqixl4niQU1gvb5WpmMi6epwMWPod3t6p98zvb51w6R/GWv.v/	root	SHA-512	TRUE	TRUE	['sample C3.zip', 'VSWd2/NVMe/docker/overlay2/5814e9f668e8255d628f9b300a1eb7000f153a70f53e39c2b9c749fbd640d20f/diff/cu alluse.tar.bz2', 'etc/shado
	zte		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5b0a50b2d9c2aeee819bcdbfb5eac640b7af876c4f8062F4a9d584bc7e090a3f/diff/etc/passwd-]
	root		FALSE		[sample_C3.zip], VSWd2/NVMe/docker/overlav2/5b0a50b2d9c2aeee8196cdb7b5eac640b7af876c4f8062f4a9d584bc7e090a3f/diff/etc/passwd-7
	zte		FALSE		[sample_C3.zip]. VSWd2/NVMe/docker/overlav2/5127328289b7bad3f65b4e425a2bde89d2fb7b3ad247b25c086baae3ea4a192b/diff/etc/passwd-1
	root		FALSE		[sample_C3.zip], VSWd2/NVMe/docker/overlag/2/5f27328289b7bad3f65b4e425a2bde89d2fb7b3ad247b25c086baae3ea4a192b/dlff/etc/passwd-]
	zte		FALSE		[sample_C3.zip] v5wd2/NVMe/docker/overlay2/6/09988d35b34d0ead041c7a8f15926213fabd0418ef4244eb4f3dca5420e/diff/etc/aassw/]
	root		FALSE		
	root		FALSE		[sample_3.zip], VSWd2/NVMe/docker/overlay2/60309898d35b34d0ead041c7la8f15926213fab6d9d18ef4244eb4f3dca5420e/diff/etc/passwd-]
	zte		FALSE		[sample_3.zip], v3w02/NVMe/docker/overlay2/630358580350540eab641c/nasi35202131a0605036614244654150028406/gith/etc/passwd-] ['sample_C3.zip', VSWd2/NVMe/docker/overlay2/62d4399f5bca8b789797457a0a1fd4edd1f03ce8b6544ce83c4335ee839d851c/diff/etc/passwd-']
	root		FALSE		
	zte		FALSE		['sample_C3.zip', VSWd2/NVMe/docker/overlay2/62d4399f5bca8b789797457a0a1fd4edd1f03ce8b6544ce83of335ee839d851c/diff/etc/passwd-'] Fsample_C3.zip', VSWd2/NVMe/docker/overlay2/65aed621c1373324fd5aab438f892a2942efe3036159ca31dd12760fb0249b80/diff/etc/passwd-']
			FALSE		[sample_L3.zip, VSW02/NVMe/docker/overlay2/65aed621c1373324fd5aab438f892a2942efe3036159ca31dd12/60fb0249b80/diff/etc/passwd-] ['sample_C3.zip', VSWd2/NVMe/docker/overlay2/65aed621c1373324fd5aab438f892a2942efe3036159ca31dd12760fb0249b80/diff/etc/passwd-']
	root				[sample_C3.zip", VSWd2/NVMe/docker/overlay2/d5aedb22c13/5524rd5aacb4str852a2942ere/sisb19Ca31dd12/d0rd0249880/diff/etc/passwd-] ['sample_C3.zip", VSWd2/NVMe/docker/overlay2/dc442e253ced7974b143eb239b964620d93660671c1a6da287dbc2e8ec714396/diff/etc/passwd-']
	zte		FALSE		
	root		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/6c442e253ced7974b143eb239b964620d93660671c1a6da287dbc2e8ec714396/diff/etc/passwd-']
	zte		FALSE		['sample_C3.zip', VSWd2/NVMe/docker/overlay2/6c48317a4046411ed381d152dta94a54ae2ac1be608a2e67747b4617b65d380f/diff/etc/passwd-']
	root		FALSE		['sample_C3.zip', VSWd2/NVMe/docker/overlay2/6c48317a4046411ed381d152dca94a54ae2ac1be608a2e67747b4617b65d380f/diff/etc/passwd-']
	root		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75080e74e03ac9855d59c8d4cf185b2580dcf5ab37b23187acb309f2a2cd0cef/diff/etc/passwd']
	zte		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/7e5644095eea125b7396dc056da0465f18d035ce2ce87a7875b9a3ac8683b783/diff/etc/passwd-']
	root		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/7e5644095eea125b7396dc056da0465f18d055ce2ce87a7875b9a3ac8683b783/dlff/etc/passwd-']
	zte		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8292a480177739b9c6cc3dd4a7f86627211b02554fd9ed06b5e1a9fbb9980766/diff/etc/passwd-7
	root		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8292a480177739b9c6cc3dd4a786627211b02554fd9ed06bSe1a9fbb9980766/diff/etc/passwd-']
	root		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/831d1aa8a958adf2652f85b2b24e49396f0c4cce755f67927342f33086ae346b/diff/etc/passwd']
	zte		FALSE		['sample_C3.zip', 'VSWdz/NVMe/docker/overlay2/84a203fa8bef7c6b26ea27d34184c20707252372bc4cd012bc6672a9692d1d3f/diff/etc/passwd-']
	root		FALSE		['sample_C3.zip', VSWd2/NVMe/docker/overlay2/84a203fa8bef7c6b26ea27d34184c20707252372bc4cd012bc6672a9692d1d3f/diff/etc/passwd-']
	zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8930095eb00c45686268156012d1c890433d4812ba0b288bc5634db521204373/diff/etc/passwd']
	root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8930095eb00c45686268166012d1c890433d4812ba0b288bc5634db521204373/diff/etc/passwd']
	root		FALSE	FALSE	['sample_c3.zip', 'VSWd2/NVMe/docker/overlay2/8930095eb00c45686268166012d1c890433d4812ba0b288bc5634db521204373/diff/etc/passwd-']
	root		FALSE	FALSE	['sample_c3.zip', 'VSWd2/NVMe/docker/overlay2/5181742d686a025499e4d8a785b50561df43dcda0b1f4bbbbbbb23429d9740985/diff/etc/passwd']
	root		FALSE	FALSE	['sample_C3.rip', 'VSWd2/NVMe/docker/overlay2/9181742d686a025499e4d8a785b50561df43dcda0b1f4bbbb0b23429d9740985/diff/etc/passwd-']
	zte		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/96b11ead8e7b31bdf877093871B44aa3188b0b40:9df2300bc8d06a399259654/diff/etc/passwd']
	root		FALSE		['sample_C3.zip', 'VSWd2/NVMe/docker/overlav2/96b11ead8e7b31bdf877093871844aa3188b0b40c9df2300bc8d06a399259654/diff/etc/passwd']
	root		FALSE		[sample_C3.zip], VSWd2/NVMe/docker/overlav2/96b11ead8e7b31bdf877093871844aa3188b0b40c9df2300bc8df6a399259654/diff/etc/passwd-1

Figure 83; C3 Infoleak passwords (Black Duck)

A	8	C
Url	File	Domain
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bsa/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/config.v2.json']	Unknow
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/lrrm-sub1g/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db8a745fa3174a6194ca831a2bb46fa7a09ae70dee169/config.v2.json']	Unknov
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/e2c/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/config.v2.json']	Unknov
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/dia/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']	Unknov
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/de1m/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']	Unknov
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cis-modb/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0ad9b0ee06c38f37939e01abd51dcf6e811526f76b97427ea3b206d68d949d5f/config.v2.json']	Unknov
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bcs-modb/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/13639ffc18e25a32ffef1b1721fd366dca31b977eea5e80586384a235ab77c70/config.v2.json']	Unknow
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/swm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/142e539193a5fe6332e8eb792fbd2b2844be84570de50441edcfc1391e82d154/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/umftaskmanager/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/15627663defbc22a944279a54ff1033784d007d5bd054e7dbc99fa87eb29035e/config.v2.json']	Unknor
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cos/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/16895a4cf185fd7b66e00f2817a336323c7f46da85059336864624b0cef1b972/config.v2.json']	Unknor
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/uds_0/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/180529292a014b2bbaa010b3a1910b79b1d833448cabf92e3e3d172389d0ff46/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bum/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/18b36be7cd13196dee7719964ba2ee308bdbea16f079d37b4b989de24e96027a/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/lcs/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/18c34d8253c58d1eb9ece098f375e7557a55102143fbcf1e520d94348097a15c/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/hia/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/194fce24e46157670e1f3550aa50114683644b779aa0035e28fb27cbdd6bcd12/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bf1m/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/1a69d88d9ef3bf5a3f7491627a9c9e61a64eca262ad63733c7e338021030de2e/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/certm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/1cae544de62ce54a36263c93ec9cc85e09d138e4e7e0ab4ae5ee2fa4b5a3ed6d/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/mim/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/216f9a2685f2751c5f49976416fbe8015e986ca1709c343b604986300a353879/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/log/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/26edb62455b95f1dfba90e6ae009a360d0ce22df7a1f7416f35b211d24faf458/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/anr/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/28b58634da9522104f82960015694d1f0379ab54ad6c222958f2a0479f05055e/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/webmnt/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/2b7b8c58aa7370399391254397d7454b5925336f67c55d124e548d1d73649c40/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/ucs-modb/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/39c6d6e73f382a37b04028fb5baea67514fee2ed74296744744539d0a212d92a/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/ro/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/3adb4702e0b85539d2225f262263d775eafb2f7ef22765233e78c0fe34f77a0d/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/dpf-dts/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/3cc4107a2b0877166f707cbf1727fd727e2cff4fb98575625a753588c5be231c/config.v2.json']	Unkn
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/lucm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/3d4c12504e669a59306d07a112e7567d61ec1e4a2efdb75520d5f4673642d639/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/sctp-ng/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/4285afbd02914e7d607c67245338556eb1faa87b08204f74734ab92e0edbe911/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/cpf-dts/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/43a8d110aa848a4f82efbce6a1814e1ca6ee1fed8685963725126b9269da4a36/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/cocs/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/4452a7d0ef9d10796b0c55abe8f57a4f5bdaa38b6390037bd067cca188af0713/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/nrdbs/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/4523b5aeec84cf70abfecf3057bd0f5d07426a51f2e7e9644be9d310c263be2a/config.v2.json']	Unkn
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/tcfs/pods/0	['sample C3.zip', 'VSWd2/NVMe/docker/containers/474cd235f9492e3e4ae1bcbded71d234f6e12d4e6e0ade49594b846e48da6949/config.v2.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/xnm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/51bf6c522934ff77fc738cdbf99a323c66f86348446b3b2083187aefd900d415/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/ngm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/532fd8885193614176394d4f8cef70176919a4686606f51d3a541b59e8fd287b/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/Irrm-hf/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/55ce51e14bcbd94328bb232daee49e01bf854a27116cdd3d1fcc577723d7fb6c/config.v2.json']	Unkn
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/xnsc/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/563fd0a942325f6d992b9174f42a36256f9f70b7164991628bac915016124473/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/rum/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/5ab0643f79d16a1d5087fc058ea6bf4abe52d4c48484685732dbf7b778dc986d/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/luc/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/600174e69dae35774bac4fd39f5eb75eba9a4486bdb6f6149c5f8cfc005e5a71/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/ids/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/7016bd9c8ae1d65e80747b70ae0bd553174adcc139eb5d2bdb3ce9ec3b10ae31/config.v2.ison']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/ce1m/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/755df704aa92cb10974073816ad5dc48a7630ecb6c9bdf68f3058f43ebcc296d/config.v2.json']	Unkno
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/hccm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/7acc760bee15237ec439869d1d3a5b35f6fcaaffb19d0b2fb7f88c6eea6e4433/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/weblmt/pods/0	['sample_C3.zip', VSWd2/NVMe/docker/containers/7bb0268e7dd6c23cd85ce6e4e06b0527c735dbf14de04a3c5e606b63c13f9c5b/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/docs/pods/0	['sample_C3.zip', VSWd2/NVMe/docker/containers/7effae9e2319ee8ce925177aa478602cd8586219f6c72d9a1264e130168e439f/config.v2.json']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/nf-oam/pods/0	['sample_C3.zip', VSWd2/NVMe/docker/containers/83b95f4af68a3e066562371b5858736527d1a88f81fbdd75bbee5bf57d611170/config.v2.ison']	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/rse/pods/0	[sample_C3;io], VSWd2/NVMe/docker/containers/84b68220f590ac62563265202e66fd7986a5f53aebbe43710a58a032c1519f1f/config-v2;ion]	Unkn
ttp://192.254.1.16:8098/api/v1/namespaces/1/rcs/pci/pods/0	[sample_C3.pb, VSWd2/NVMe/docker/containers/860922485bd1313729bb006cb22a6dea2d33fte74b0647a69de2b725841/config.v2.json] [sample_C3.pb, VSWd2/NVMe/docker/containers/860922485bd1313729bb006cb22a6dea2d33fte74b0647a69de2b725841/config.v2.json]	Unkn
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/pci/pcds/0	[sample_52:p]; vswdz/vvwe/dccer/containers/8e0922483bdte13137213bb0bbbcd2228bteazct3112740bd47858de227228447comg.v2.json] ['sample_C3.zip', 'VSWd2/NVMe/dccker/containers/8e0010d69031e664afeb724d9414474b3259bce12bf4ec51ada3bd524728bb3b/config.v2.json']	Unkn
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/mdc/pods/0	[sample_cs.zip', vswdz/www/dcker/containers/8f89a05559d91113ac33f6a57920951eccd50f98ce688a03c18767ae211b2112/config.vz.json']	Unkno
http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cins-modb/pods/0	[sample_cs.zip], vswdz/www.docker/containers/96041ac3a811d245233558e5f3f93c92b675fa3681295dd3342d182e5cbe18d2/config.vz.json]	Unkno
< C3 infoleak-urls +	[ sumple_costs), sources(contacts) sources(contacts) sources(contacts) sources(contacts) and a sumple costs) and a sumple cost of the sum of th	i

Figure 84: C3 Infoleak URLS (Black Duck)

omponent lask	Version 1.1.1	2.2.2	r CVE Matching type CVE-2023-Exact match	CV55 CVE publicObject compilation dat 1.7 2023-05-0-2021-08-25T11-41:46Z	flask.app.pvc	Object full path Object 5HA1 CV sample C3.ztp://SWd2/NVMe/docker/over c130215837e768	553 CVSS vect CVSS vect Summary Distributii CVSS (Dist CVSS) (Di Triage vec Unresolvi Note type Note i 6.5 AV:N/AC:J/PE:N/UEN/SSJ/C-W/EN/A:J/IE:U/IE:O/IR:CC	eas Vulnerabi Missing ei 805A Version override type http://red.nist.eov/ 805A-2023-3080
lask	1.1.1	2.2.2	CVE-2023-Exact match					http://wd.nist.gov/ 8054-2023-1080
isk isk	1.1.1	2.2.2	CVE-2023-Exact match	3.7 2023-05-0 2021-08-25711:41:462 1.7 2023-05-0 2021-08-25711:41:462	flask.app.pyc flask.app.pyc	sample_C3.zip:V5Wd2/NVMe/docker/overc110215837e768 sample_C3.zip:V5Wd2/NVMe/docker/overc110215837e768	6.5 AV:N/AC:U/PR:N/U:N/S:U/C:P/I:N/A:N/E:U/R::O/RC:C 6.5 AV:N/AC:U/PR:N/U:N/S:U/C:P/I:N/A:N/E:U/R::O/RC:C	http://wd.nist.gov/ 8054-2025-2080 http://wd.nist.gov/ 8054-2023-2080
18	111	2.2.2	CVE-2023-Exact match	3.7 2023-05-0-2021-08-23711-41/462	flask.app.pyc	sample_CLID:/VSW02/WVMe/cocker/overcli0215837e766 sample_C3.zip:/VSW02/WVMe/registru/docc100215837e766	<ul> <li>6.5 AV:N/ACU/PEN/UER/SU/CH/IN/AIN/EU/RED/RCIC</li> <li>6.5 AV:N/ACU/PEN/UER/SU/CH/IN/AIN/EU/RED/RCIC</li> </ul>	http://wd.nist.gov/ 8054-2023-1080 http://wd.nist.gov/ 8054-2023-1080
sk ck	111	2.2.2	CVE-2023-Exact match	1.7 2023-05-0 2021-08-25111-41:462 3.7 2023-05-0 2021-08-25111-41:462		sample_C3.210:V5W02/WVMe/registry/doc t110215837e760 sample_C3.210:V5W02/WVMe/registry/doc t120215837e760		http://wd.nist.gov/ 6054-2023-2080 http://wd.nist.gov/ 6054-2023-2080
	111	2.2.2	CVE-2023-Exact match		flask.app.pyc			http://wd.nist.gov/ 8054-2023-1080 http://wd.nist.gov/ 8054-2023-1080
sk sk	1.1.1	2.2.2	CVE-2023-Exact match CVE-2023-Exact match	3.7 2023-05-0-2021-08-25111-41:462 3.7 2023-05-0-2021-08-25111-41:462	flask.app.pyc flask.app.pyc	sample_C3.zip/V5Wd2/NVMe/ssd/1/versic c138215837e768: sample_C3.zip/V5Wd2/NVMe/ssd/1/versic c138215837e768	6.5 AV:N/ACI//PR:N/UEN/SIJ/CH/EN/AEN/EU/REI/RCIC 6.5 AV:N/ACI//PR:N/UEN/SIJ/CH/EN/AEN/EU/REI/REI/RCIC	http://wd.nist.gov/ 6054-2023-1080 http://wd.nist.gov/ 6054-2023-1080
h .		5.2.15	CVE-2018-Exact match	10 2014-09-2(2019-02-2)111-41-462	bash	sample_C3.pp:V5Wd2/WVMe/docket/over 79151d52932629	6.5 AVEN/ACL/MEN/UCH/SN/CH/EN/ACN/ED/ACL/MCSC 0 AVEN/ACL/Aurn/C/C/I/C/A/C	http://weinis.gov/scise-2025-2080
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-21 2019-02-21 10:51:522 10 2014-09-21 2019-02-21 10:51:532	bash	sample_C3.21p:VSW02/WVMe/docket/over 79151d529126391 sample_C3.21p:VSW02/WVMe/docket/over 79151d529126391	0 AV:N/ACIJAUN/CC/NC/AC	http://wino-pie, no-immediate-binding
h h		5.2.15	CVE-2014-Exact match	10 2014-09-212019-02-21110-311332	bash	sample_C3.zip.VSWd2/NVMe/rd2CKer/over /9131d52912639	0 AVN/ACL/ALN/CC/IC/AC	http://wino-pie, no-immediate-binding
	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-212019-02-21110/51/532	bash	sample_Cs.bp.vswb2/wvwe/registry/doc /91318524282835 sample_C3.zip.v5Wd2/WvWe/ssd/1/zwm/ 79151d529326391	0 AVN/ACUAEN/CO/OC/AC 0 AVN/ACU/AEN/CO/OC/AC	http://wi.no-pie, no-immediate-binding
h h	4.2.50	3.2.15	CVE-2014-Exact match	10 2014-05-2 2015-02-21112-03:552	bash	sample_C3.rtp/VSWd2/WVMe/ssd/1/versic ta35450cf900223	0 AVN/ACIJALIN/CC/VC/AC	http://wirno.pie, no-fortify-source, no-stack-protected, no-immediate-binding, no-
h	4.2.50	5.2.15	CVE-2014 Exact match	10 2014-09-21 2021-01-26716-32:012	bash	sample_C3.pp.V5Wd2/WVMe/ssd/1/versic 3712a04af21435c	D AV:N/AC:L/AU:N:/C:C/UC/A:C	http://wino pie, no romey source, no sauce protected, no immediate binding, no- http://wino stack-protected, no-pie, no-immediate-binding, no-fortify-source
6	4.2.50	3.2.15	CVE-2014-Exact match	10 2014-09-21 2021-01-20110-12:012	besh	sample_C3.rtp:V5Wd2/TuffOrive/Partition_3712a04af21435c	0 AV/N/ACU/AUN/CC/NC/AC	http://wino-stack-protected, no-pie, no-immediate-binding, no-fortify-source
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-21 2021-01-20110:5125012	bash	sample_CLIP/VSWB2/TuffDrive/Partitiony 79151d52932639	0 AV/N/ACIL/AUNI/CIC/VC/AIC	http://wcno.siex-protected, no-pie, no-immediate-dividing, no-romy-source http://wcno.pie, no-immediate-binding
sh .		3.2.15	CVE-2014-Exact match	10 2014-09-212019-02-21110:31:552	bash	sample_CL2ip/SWd2/TuffDrive/Partitions 79151d52912638	6 AV N/ACL/AUN/CC/AC	http://weino.pie.no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-21 2019-02-21110-51:532	bash	sample_CLIP_VSW02/VUMe/docker/over 79151d52932639!	0 AVN/ACL/ALIN/CL/NC/ALC 0 AVN/ACL/ALIN/CL/NC/ALC	http://wi.no-pie, no-immediate-binding
b.	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-21 2019-02-21110-31:532	bash	sample_C3.zig/VSWd2/NVMe/docker/over 79151d52932659.	D AV/N/ACIJ/ALN/CC/IC/AC	http://wcno-pie, no-immediate-binding
h	42.50	52.15	CVE-2014-Exact match	10 2014-09-2:2019-02-21710-51:532	hash	sample_C3.zip.V5Wd2/NVMe/registru/doc 79151d52932639	0 AV:N/AC:L/Au:N:/C:C/UC/A:C	http://wcno.pie, no-immediate binding
n n	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2:2019-02-21110-51:552	hash	sample_C3.2(p.V3Wd2/WVWe/registry/dic /9131d52932639) sample_C3.2(p.V3Wd2/WVWe/sid/1/sam/ 79131d52932639)	0 AV:N/ACU/AUN/CC/VC/AC	http://winopie.no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2/2019-02-21112-03:252	bash	sample_C3.pp.VSWd2/NVMe/ssd/1/versic 6a38460cf900223	0 AV/N/ACIU/AUN/CIC/VC/AIC	http://wino.pie, no-fortify-source, no-stack-protected, no-immediate-binding, no-
h	4.2.50	5215	CVE-2014-Exact match	10 2014-09-2/2021-02-23112-08/252 10 2014-09-2/2021-01-26716:32:012	bach	sample_C3.pp.VSW02/WVWe/s50/1/Versic 005000000025 sample_C3.pp.VSW02/WVWe/s50/1/Versic 5712a04af21435c	0 AV:N/ACI/AUN/CC/ICC/AC	http://witho.pie, no roriny source, no stack protected, no immediate binding, no- http://witho.stack-protected, no-pie, no-immediate-binding, no-fortify-source
h	4.2.50	3.2.15	CVE-2014-Exact match	10 2014-09-21 2021-01-2018-12:012	bash	sample_C3.ztp:VSWd2/TuffDrive/Partition.3712a04af21435c	6 AVN/ACUALN/CC/IC/AC	http://weno-stack-protected, no-pe, no-immediate-binding, no-fortify-source
b	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-21 2019-02-21 710-51:532	bash	sample_C3.zip.VSWd2/TuffDrive/Partitionv 79151d52932639	0 AV:N/ACI/AuN:/CC/I/C/A/C	http://wcno-pie, no-immediate-binding
h		5.2.15	CVE-2014-Exact match	10 2014-09-2:2019-02-21710-51:532	bash	sample_C3.zip.VSWd2/TuffDrive/Partition/ 79151d52932639	0 AV9/ACU/AutN/CC/bC/AC	http://wcno-pie, no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2 2019-02-21710-51:522	bach	sample_Cs.2p.VSWd2/NVMe/docker/over 79151d52932639	0 AV/N/ACIU/AUN/CIC/UC/AIC	http://w.no-pie, no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2 2019-02-21110-31:532	bash	sample_C3.rtp:V5Wd2/NVMe/docker/over 79151d52912639	D AV N/ACI/AuN/CCI/CCAC	http://www.no-me.no-immediate-binding
h	42.50	52.15	CVE-2014 Exact match	10 2014-09-2 2019-02-21110-31:532	bach	sample_Casip/viviag/wwweptocceptorel/statisticspages	0 AV:N/AC:L/AU:N:/C:C/I:C/A:C	http://wcno.pie, no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exect match	10 2014-09-2 2019-02-21110-51:537	hash	sample C3.stp:V5Wd2/NVMe/ssd/1/sum/ 79151d52932639	D AV:N/AC:L/Av:N:/C:C/I:C/A:C	http://wino.pie.no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2 2021-02-23712:03:232	bash	sample_C3.zip:V5Wd2/NVMe/ssd/1/versic 6a38460cf900223	0 AV:N/ACIJ/Au:N:/CIC/I/C/AIC	http://wino.pie, no-fortify-source, no-stack-protected, no-immediate-binding, no-i
h	42.50	3.2.15	CVE-2014-Exect match	10 2014-09-3 2021-01-26716:12:017	bash	sample_CL:rp:VSWd2/NVMe/ssd/1/versic3712a0faf21435c	0 AV:N/AC:L/Au:N:/C:C/L/C/A:C	http://mcno-stack-protected, no-pie, no-immediate-binding, no-fortify-source
8	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2 2021-01-26716-32:012	bash	sample_C3.zip/VSWd2/TuffOrive/Partition_3712a04af21435c	0 AV:N/AC:UAu:N/CC/I/C/A/C	http://weno-stack-protected, no-pie, no-immediate-binding, no-fortify-source
0	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2 2019-02-21110-31:532	bash	sample C3.10/VSWD/TuffOrive/Partition 79151d52912639	0 AV:N/AC:L/Au:N:/C:C/I:C/A:C	http://www.no-size-projected, no per, no initial date unong, no rorary source
h	42.50	\$2.15	CVE-2014 Exact match	10 2014-09-2 2019-02-21710-51:532	bach	sample_C3.zip.VSWd2/TuffDrive/Partition: 79151d52932639!	0.8V%/AC1/Au%/CC/I/C/A/C	http://wcno.pie, no-immediate-binding
n n	4.2.50	5.2.15	CVE-2014 Exact match	10 2014-09-2 2019-02-21110-31:522	hash	sample_C3.0p.V3W02/Y0H0H0H0/PartitionC79131052932659. sample_C3.0p.V3W02/NVMe/docker/over 79131d52912639	6 AV/N/ACIUALIN/CC/NC/AC	http://wino.pee.no-immediate-binding
h		5.2.15	CVE-2014-Exact match	10 2014-09-3 2019-02-21710:51:532	bash	sample_C3.zip/VSWd2/WVMe/docker/over 79151d52932639	0 AV:N/AC:L/Au:N(CIC/UC/AIC	http://wino.pie, no-immediate-binding
ð	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-10 2019-02-21110-31:552	bach	sample_C3.2p.V5Wd2/WVMe/realstru/doc 79151d52912639	0 AV:N/AC:UAUN/CC/ICC/AC	http://withopie.no-immediate-binding
h	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-11 2019-02-21710-51:532	bash	sample C3.zip/VSWd2/NVMe/std/1/sum/ 79151d52912639	0 AVM/ACIJ/AUN/CIC/I/C/A/C	http://neroo.pie.no-immediate-binding
h	4.2.50	3.2.15	CVE-2014-Exact match	10 2014-09-3 2021-02-23112:03:232	besh	sample_C3.zip.V5Wd2/N/Me/ssd/1/versic 6a36460cf500223	0 AV:N/ACIJ/AuN:/CC/I/C/A/C	http://www.no-pie.no-fortify-source.no-stack-protected.no-immediate-binding.no-
h.	4.2.50	5.2.15	CVF-2018-Exact match	10 2014-09-3 2021-01-26736:32:012	bash	sample_C3.zip.V5Wd2/WVMe/ssd/1/versic37[2s04af2]435c	0 aven/acti/acti/cc/irc/act	http://wirno-stack-protected, no-pie, no-immediate-binding, no-fortify-source
b	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09 1/2021-01-2010-32-012	bash	sample_C3.zig/VSWd2/TuffDrive/Partition_3712a04af21435c	0 AV NACIJAUNICICIUS/AC	http://weno-stack-protected, no-pie, no-immediate-binding, no-fortify-source
		5.2.15	CVE-2014-Exact match	10 2014-09-3/2019-02-21710-51:532	bash	sample C3.zip/VSWd2/TuffDrive/Partition 79151d52932639	0 AVN/ACL/AUN/CC/ICC/AC	http://wcno-pie, no-immediate-binding
h	42.50	52.15	CVE-2014-Exact match	10 2014-05-3(2015-02-21110-51:532	hach	sample_Cs.zip.vSwd2/TuffDrive/Partition/79151d52932639	0 AV:N/AC:L/AUNI/C:C/II:C/AIC	http://wcno-pie, no-immediate-binding
da .	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-05-3 2015-02-21110-51:522	bash	sample_C3.rtp/VSWd2/NVMe/docker/over 79151d52912639	6 AV/MACIUALINICCINC/AC	http://wcno.pie.no-immediate-binding
sh	4.2.50	52.15	CVE-2014-Exact match	10 2014-09-2 2019-02-21110-51:522	bash	sample_Ca.htp://swidz/w/wei/docker/over 79151d52932639: sample_C3.zip/VSWd2/NVMe/docker/over 79151d52932639:	0 AV:N/ACIJAUN/CC/IIC/AC	http://weno.oie.no-immediate-binding
un un	4.2.50	5.2.15	CVE-2014-Exact match	10 2014-09-2 2019-02-21110-31:552	besh	sample_CL:pp:YSWd2/WVMe/registru/doc 79151d52912639	0 AV9/ACUALN(CC/IC/AC	http://wenopie.no-immediate-binding
-		5.2.15 terabilities	PAG. WAA. GPREL WIRCOM	an analysis (019-02-2110/34/36)	VEST	sembal re-th-count acceluelingingions torrangeous	a we when the state of the stat	univities on the measurements and the

Figure 85: C3 CVEs (Black Duck)



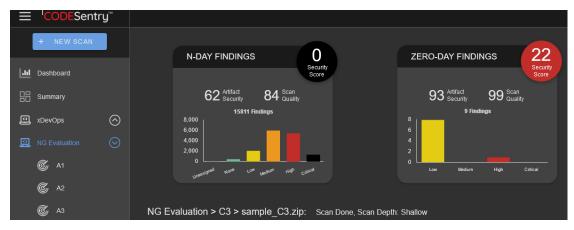


Figure 86: C3 Scan Overview (Code Sentry)

# GRAMMATECH

# <sup>I</sup>CODESentry<sup>-</sup>

# **N-Day Findings Summary**

Name	Version	Vendor	Security Score	Number of Vulnerabilities	Path
abseil	0~20200225.2	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ d7cc9189a6da87d7c25d 6b1a85a3a662c0968d45 74c605cca18b3f92a1b8e69d/diff/lib/ libadlik_serving.so
abseil	0~20200225.2	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/registry/docker/docker/ registry/V2/blobs/sha256/4c/ 4ctdbc31c66f53f0fa85cf0d62fb6a e00c2aae20241ecf4b034aa332320e fda0/data
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 0c224b9e36240bea2af020051a342f 2cc35ec58864d7702aabb71f82cd58 7e88/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 0c224b9e36240bea2af020051a342f 2cc35ec58864d7702aabb71f82cd58 7e88/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overIay2/ 0c42b43180e215ff0a52404b628202 711ba51af16e17514d946e53260a69 c0b8/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 146be2cd8110b5aeb310c988eef8ad 974a9881311868f531acb2b18db975 c1ad/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 496a068cf5f40ebf1c53923733574f 8499f8b843172a00c89ae15ef1256f cbe1/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 496a068cf5f40ebf1c53923733574f 8499f8b843172a00c89ae15ef1256f cbe1/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 60309898d35b34d0ead041c7fa8f15 926213fab6d9d18ef4244eb4f3dca5 420e/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 876db3a77b236e035d4131e9bec65c f1da8ca15f7c4fd38252110c787bd8 25a0/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/ VSWd2/NVMe/docker/overlay2/ 8930095eb00c45686268 166012d1c890433d4812 ba0b288bc5634db521204373/diff/ ordinaryuserhome/setfacl

Page 2 / 1216

www.grammatech.com

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 87: C3 N-day findings (Code Sentry)



<sup>I</sup>CODESentry<sup>-</sup>

**N-Day Findings** 

Findings for sample\_C3.zip

Scan Depth: Shallow MD5: 006198a09104c8f5f197a5407512ec8b Number of Vulnerabilities: 15811

### linux\_kernel [linux] 4.19.82

 Match Level: High

 Security Score: 0

 Path: NG Evaluation/C3/sample\_C3.zlp/VSWd2/TuffDrive/Partition4/ramdisk.bin

 Component ID: 9967864f-5b3b-4a68-820f-9ee6006dd6ac

 Score Distribution: 
 <sup>(2)</sup> Unassigned: 0
 <sup>(2)</sup> None: 26
 <sup>(2)</sup> Low: 267
 <sup>(2)</sup> Medium: 813
 <sup>(3)</sup> High: 462
 <sup>(2)</sup> Critical: 35
 <sup>(3)</sup>
 <sup>(3)</sup>
 <sup>(4)</sup>
 <sup>(4)</sup>

Severity	Score	CVSS Version	Vulnerability ID	Description
Critical	10	2.0	24041	Linux Kernel rndis.c OID_GEN_SUPPORTED_LIST Memory Corr
Critical	10	2.0	48120	Linux Kernel video4linux (V4L) uvcvideo uvc_driver.c uv
Critical	10	2.0	49957	Linux Kernel libertas Subsystem drivers/net/wireless/li
Critical	10	2.0	51253	Linux Kernel sctp net/sctp/sm_statefuns.c FWD-TSN Chunk
Critical	10	2.0	61788	Linux Kernel drivers/net/e1000e/netdev.c Ethernet Frame
Critical	10	2.0	67243	Linux Kernel fs/nfsd/nfs4xdr.c NFS XDR Compound Request
Critical	10	2.0	67896	Linux Kernel L2TP drivers/net/pppol2tp.c pppol2tp_xmit
Critical	10	2.0	74679	Linux Kernel Bluetooth net/bluetooth/l2cap_core.c l2cap
Critical	10	2.0	93755	Linux Kernel drivers/target/iscsi/iscsi_target_paramete
Critical	10	2.0	104658	Linux Kernel /netfilter/nf_conntrack_proto_dccp.c DCCP
Critical	10	2.0	107650	Linux Kernel hugetlb_entry Callback Handling Unspecifie
Critical	10	2.0	122243	Linux Kernel OZWPAN USB Host Controller Driver ozhcd.c
Critical	10	2.0	122244	Linux Kernel OZWPAN USB Host Controller Driver ozusbsvc
Critical	10	2.0	137359	Linux Kernel drivers/usb/usbip/usbip_common.c usbip_rec
Critical	10	2.0	148130	Linux Kernel nf_ct_frag6_queue() Function IPv6 Packet D
Critical	10	2.0	156288	Linux Kernel drivers/net/macsec.c macsec_start_xmit() F
Critical	10	2.0	179535	Linux Kernel drivers/char/random.c crng_ready() Functio
Critical	9.8	3.0	205886	Linux Kernel sound/soc/codecs/wcd9335.c wcd9335_codec_e
Critical	9.8	3.0	212917	Linux Kernel drivers/net/ethernet/hisilicon/hns3/hns3pf
Critical	9.8	3.0	212918	Linux Kernel drivers/net/wireless/ath/ath6kl/wmi.c ath6
Critical	9.8	3.0	212920	Linux Kernel fs/cifs/smb2pdu.c SMB2_write() Function re
Critical	9.8	3.0	212921	Linux Kernel fs/cifs/smb2pdu.c SMB2_read() Function req
Critical	9.8	3.0	212942	Linux Kernel drivers/net/wireless/rsi/rsi_91x_mac80211
Critical	9.8	3.0	212953	Linux Kernel kernel/trace/trace.c allocate_trace_buffer
Critical	9.8	3.0	218237	Linux Kernel drivers/net/wireless/marvell/mwifiex/sta_i
Critical	9.8	3.0	218239	Linux Kernel drivers/net/wireless/marvell/libertas/cfg
Critical	9.8	3.0	226740	Linux Kernel drivers/input/input.c input_default_setkey

www.grammatech.com

Page 223 / 1216

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 88: C3 Vulnerabilities (mapped to CVEs in the report) (Code Sentry)



# <sup>I</sup>CODESentry<sup>-</sup>

# **Zero-Day Findings**

## Findings for sample\_C3.zip

Scan Depth: Shallow MD5: 006198a09104c8f5f197a5407512ec8b

### Top 25 CWE Findings

Rank	ID	Name	Instances
1	CWE:787	Out-of-bounds Write	-
2	CWE:79	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	-
3	CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0
4	CWE:20	Improper Input Validation	-
5	CWE:125	Out-of-bounds Read	-
6	CWE:78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0
7	CWE:416	Use After Free	0
8	CWE:22	Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")	-
9	CWE:352	Cross-Site Request Forgery (CSRF)	-
10	CWE:434	Unrestricted Upload of File with Dangerous Type	-
11	CWE:476	NULL Pointer Dereference	-
12	CWE:502	Deserialization of Untrusted Data	-
13	CWE:190	Integer Overflow or Wraparound	-
14	CWE:287	Improper Authentication	-
15	CWE:798	Use of Hard-coded Credentials	0
16	CWE:862	Missing Authorization	-
17	CWE:77	Improper Neutralization of Special Elements used in a Command ("Command Injection")	-
18	CWE:306	Missing Authentication for Critical Function	-
19	CWE:119	Improper Restriction of Operations within the Bounds of a Memory Buffer	14
20	CWE:276	Incorrect Default Permissions	-
21	CWE:918	Server-Side Request Forgery	-
22	CWE:362	Concurrent Execution using Shared Resource with Improper Synchronization ("Race Condition")	-
23	CWE:400	Uncontrolled Resource Consumption	-
24	CWE:611	Improper Restriction of XML External Entity Reference	-
25	CWE:94	Improper Control of Generation of Code ("Code Injection")	-

## All Other CWE Findings (Excluding Top 25 CWEs)

Severity	Score	CWE ID	Name	Instances
Low	2.83	CWE:328	Reversible One-Way Hash	161
😣 Low	2.83	CWE:242	Use of Inherently Dangerous Function	14
Low	2.83	CWE:676	Use of Potentially Dangerous Function	391
Low	2.83	CWE:327	Use of a Broken or Risky Cryptographic Algorithm	161
Low	0.2	CWE:326	Inadequate Encryption Strength	19

www.grammatech.com

Page 864 / 1216

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 89: C3 Zero-day findings (Code Sentry)

# Sample C3 Jarvis Scan Report Excerpts

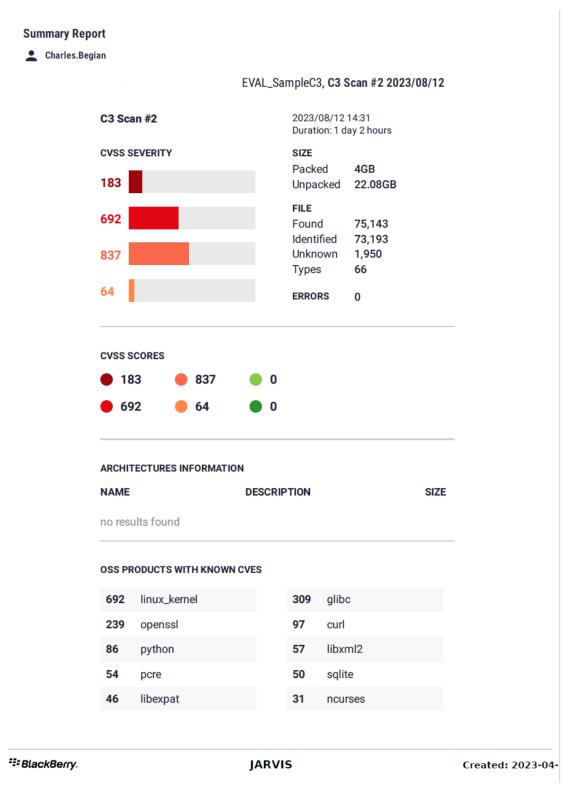


Figure 90: C3 Scan Overview (Jarvis)

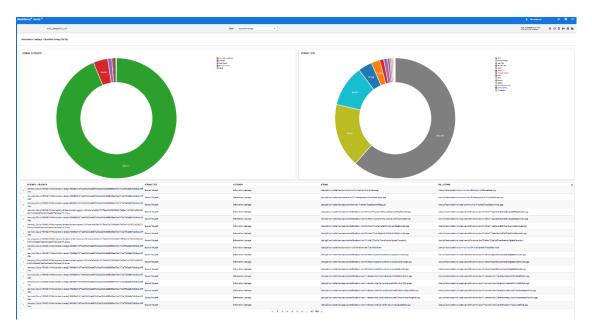


Figure 91: C3 Information Leakage (Jarvis)

BlackBerry <sup>®</sup> Jarvis <sup>®</sup>			🛓 Charle	Begian		荘	?	₽
EVAL_SampleC	l→C3 View	CVEs .	10.31 12-08-2023 (tor Scanned by Charles B	1 day) gian	¢	t e	8 8	0
Third Party: CVEs								
CVSS V3.1 SEVERITY	0.37	THIRD-PARTY P	ROULCT	inux, ken opisal	m :			

## Figure 92: C3 CVSS Severity Report (Jarvis)

ackBerry <sup>®</sup> Jar	vis ®										
Scan Results	Charles.Begian@ ▼	EVAL_Sa	mpleC3 -								
COMPONENT	¢ NAME	¢ DATE	¢ CRITICAL	\$ HIGH	♦ MEDIUM	¢ LOW	¢ PACKED SIZE		IDENTIFIED	<b>≑</b> FOUND	\$ TYPES
EVAL_Sampl	C3 (02)	2023/08/12	183	692	837	64	4GB	22.08GB	73193	75143	66

# Figure 93: C3 CVE Summary by Severity (Jarvis)

A 8	C	0	E	F	G. H		ĸ	1.	0	0	R.	5	T	0 5	W.	- X	Z.	44	
ptimesta exter	wionfile_info.5NA3-512 file	info.file_name	file_info.ffile_i	info,file_type	file_info.;file_info.relativeh	as expired	issuer.common_name	Issuer country	Issuer.organi	ainot_after	not_before	private k	private_kop	ablic_ke publi	c hancen id i	alf_sign	signature_algorithm	subject.common_name	54
2023-06-1	4 052d723eef0bb52c68ef0caf3babi stee	ert.cer	/sample_(PEM	CERTIFICATE	/sample_CV5Wd2/NVMe/d	FALSE	21E Corporation Sub RSA Certificate Authority S2	CN	cull	203702160216483	202202100216482	null	FALSE	2,048	6 82483450-	FALSE	sha256WithR5AEncryption	741821400699.ste.com.on	0
2023-06-1	0 5489866cd9adee5c258466cld8bd bee	po.ert	/sample_(PEM	CERTIFICATE	/sample_thome/webmnt/i	FALSE	rull	CN	Dummy Cert	fi 202904230840532	201904200840512	mult	FALSE	2,048	6 83483450-	FALSE	sha256WithR5AEncryption	null	- 03
2023-06-1	4 052d723eef0bb52c68ef0caf3babi :tee	ert.oer	/sample (PEM	CERTIFICATE	/sample_CVSWd2/NVMe/d	FAISE	2TE Corporation Sub RSA Certificate Authority 52	CN	null	203702160216483	202202160216482	null	FALSE	2,048	6.83483450-	FALSE	sha256WithRS&Encryption	741821400099.zte.com.cn	O
3023-08-1	0 5489864cd9adee5c258414c4d8bd serv	er.ot	/sample_(PEM	CERTIFICATE	/sample_thome/webmnt/-	FALSE	null	CN	Dummy Cent	ri 202904230840513	201904260840512	null	FALSE	2,048	6 82483450-	FALSE	sha256WithRSAEncryption	null	CN
2023-05-1	4 052d723eef0bb52c68ef0caf3babizter	ert.cer	/sample_(PEM	CERTIFICATE	/sample_cvSwd2/NvMe/d	FALSE	ZTE Corporation Sub RSA Certificate Authority 52	CN.	.rull	203702160216483	202202160216482	null	FALSE	2,048	6 82483450-	FALSE	sha256WithRSAEncryption	741821400699.zte.com.on	ON
3023-08-1	4 052d723eef0bb52c88ef0caf3babizter	ert.cer	/sample_(PEM	CERTIFICATE	/sample_cvSWd2/TuffDrivi	FALSE	ZTE Corporation Sub RSA Certificate Authority 52	CN	null	203702160216483	202202160216482	nuti	FALSE	2,048	6 82483450-	FALSE	sha256WithRSAEncryption	741821400699.xte.com.cn	CN
3023-06-1	0 5489864cd9adee5c258474c4d8bd bee	to.ort	/cample_(PEM	CERTIFICATE	/sample_cv5Wd2/NetMa/d	FALSE	Rull	CN	Dummy Cert	11202904230840513	201904260640512	null	FALSE	2,048	6 82483450-	FALSE	sha256With#SAEncryption	null	CN
3023-08-1	0 5489864cd9adee5c2584F4c4d8bd serv	er.ot	/sample_(PEM	CERTIFICATE	/sample_cvSWd2/tvrMe/d	FALSE	nall	CN	Dummy Cert	fi 202904250840513	201904260840512	null	FALSE	2,048	6 82483450-	FALSE	sha256With#SAEncryption	null	CN
2023-08-1	4 052d723eef0bb52c88ef0caf3babi stee	ert.cer	/sample_(PEM	CERTIFICATE	/sample_cvSWd2/1uffDrivi	FALSE	211 Corporation Sub #SA Certificate Authority 52	CN	null	203702160216483	202202160216482	null	TALSE	2,048	6 82483435-	PALSE	sha256With#SAEncryption	741821400675.ste.com.ch	CN
2023-08-1	4 052d723eef0bb52c88ef0caf3babi.nee	erl.cer	/sample (PEM	CERTIFICATE	/sample_cv5Wd2/1uffOrtel	FALSE	2TE Corporation Sub RSA Certificate Authority 52	CN	null	203703160216483	202202100216482	null	FALSE	2,048	8 82483430-	FALSE	sha256WithE5AEncryption	741821400699.ste.com.on	CN
2023-06-1	4 052d723eef0bb52c88ef0csf3babizter	ert.cer	/sample_(PEM	CERTIFICATE	/sample_CVSWd2/NVMe/d	FALSE	ZTE Corporation Sub RSA Certificate Authority 52	CN	null	203702160216483	202202160236482	null	FALSE	2,048	6 82483450-	FALSE.	sha256WithRSAEncryption	741821400699.ste.com.on	CN
2023-08-1	4 (52d723eef0bb52c88ef0caf3babi zter	ert.cer	/sample (PEM	CERTIFICATE	/sample (VSWd2/NVMe/d	FALSE	27E Corporation Sub RSA Certificate Authority S2	CN	null	203702160216482	202202160236482	null	FALSE	2,048	\$ 83483450-	FALSE	sha256WithRS&Encryption	741821490699.tte.com.on	CN
1023-08-L	4 052d723eef0bb52c88ef0caf3babi :ter	ert.cer	/sample_(PEM	CERTIFICATE	/sample_cv5Wd2/N/Me/d	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	209702160216483	202202160216482	null	FALSE	2,048	6 82483450-	FALSE	sha256WithRSAEncryption	741821400699.ite.com.cn	CN
2023-08-1	4 052d723eef0bb52c68ef0caf3bab/zter	ert.cer	/sample_(PEM	CERTIFICATE	/sample_CVSWd2/NVMe/d	FALSE	2TE Corporation Sub RSA Certificate Authority S2	CN	null	203702160216483	202202160216482	null	FALSE	2,048	6 82483450	FALSE	sha256WithRSAEncryption	741821400699.ste.com.on	CN
2023-08-1	4 052d723eef0bb52c88ef0caf3babizter	ert.cer	/sample_(PEM	CERTIFICATE	/sample_cvSWd2/NVMe/d	FALSE	2TE Corporation Sub RSA Certificate Authority 52	CN	nut	203702160216483	202202160216482	null	FALSE	2,048	6 83483450-	FALSE	sha256WithRSAEncryption	741821400699.zte.com.on	CN
2023-08-1	4 052d723eef0bb52c88ef0caf3bab(zter	ert.cer	/sample_(PEM,	CERTIFICATE	/sample_cv5wd2/hvtMe/d	FALSE	2TE Corporation Sub RSA Certificate Authority S2	CN	null	203702160216482	202202160216482	null	FALSE	2,048	6 82483450-	FALSE	sha256WithRSAEncryption	741821400699.zte.com.on	CN
	c3_certificates +									1.4	_	_	_	_	_	-		-	

Figure 94: C3 Certificates Report (Jarvis)

A	В	C	D E	F	G	H I	1	K	L M	N	0	Ρ	Q	S	U	V	W	ХҮ	Z	
affected_o	ertain	compone	er ove. ovs. v ove. ovs. v	ave.avss	.v ove.ovss.v2.vector	cve.cvss.v cve.cvss.v	cve.cvss	v ove.ovss.v30.vector	ove.criss.v crie.cvss.v	ove.ovss	vicve.cvss.v31.vector	ove.descr	cve.name	ove.rwd_info.published_date	cve.rvd_info.updated_date	ove.rvd_info.url_ove.pri	oblem_types	ove.refere exclusion	ive exclusi	lve file
⇔1.9.0	TRUE	libssh2	5.8 medium	FALSE	AV:N/AC:M/Au:N/C:P/I:N/A:P	8.1 high	TRUE	CVSS:3.0/AV:N/AC:L/PR:N/U:R/S:U/C:H/I:N/A:H	8.1 high	FALSE	CVSS:3.1/AV:N/AC:L/P	R In libssh2	CVE-2019-17498	10/21/2019	6/12/2023	https://nvd.nist.gCWE-1	90	null	null	/sa
⇔6.3	TRUE	libtinfo	5.8 medium	FALSE	AV:N/AC:M/Au:N/C:P/I:N/A:P	7.1 high	TRUE	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H	7.1 high	FALSE	CVSS:3.1/AV:L/AC:L/PI	R: nourses 6	CVE-2022-29458	4/18/2022	2 11/8/2022	https://nvd.nist.gCWE-1	25	https://li null	null	/sa
⊂2.24	TRUE	libanl	5 medium	FALSE	AV:N/AC1_/Au:N/C:N/I:N/A:P	7.5 high	FALSE	CVSS:3.0/AV:N/ACL/PR:N/UEN/S:U/C:N/EN/AH	7.5 high	TRUE	CVSS:3.1/AV:N/AC:L/P	R res_quen	CVE-2015-5180	6/27/2017	7 2/13/2023	https://nvd.nist.gCWE-4	76	https://s null	null	
⇔2.32	TRUE	libanl	2.1 low	FALSE	AVIL/ACIL/Au:N/C:N/I:N/A:P	5.5 medium	TRUE	CVSS:3.0/AV:L/AC:L/PR:L/UEN/S:U/C:N/EN/A:H	5.5 medium	FALSE	CVSS:3.1/AV:L/AC:L/PI	R: The iconv	CVE-2020-27618	2/26/2021	1 10/28/2022	https://nvd.nist.gCWE-8	35	https://s null	null	
<2.31	TRUE	libani	6.8 medium	TRUE	AVIL/ACIL/Au:S/CIC/IIC/AIC	7.8 high	TRUE	CVSS:3.0/AV:L/AC:L/PR:L/U:IN/S:U/C:H/I:H/A:H	7.8 high	FALSE	CVSS:3.1/AV:L/AC:L/PI	R: A flaw wa	CVE-2021-3999	8/24/2022	2 2/12/2023	https://nvd.nist.gCWE-1	93	https://w null	null	
⇔2.28	TRUE	libani	5 medium	FALSE	AV:N/ACI_/AU:N/C:N/I:N/A:P	7.5 high	FALSE	CVS5:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:N/I:N/A:H	7.5 high	TRUE	CVSS:3.1/AV:N/AC:L/P	R In the GN	CVE-2018-19591	12/4/2018	3 7/9/2020	https://nvd.nist.gCWE-2	D	https://s null	null	
<=2.34	TRUE	liban	7.5 high	FALSE	AV:N/ACL/AU:N/C:P/I:P/A:P	9.8 critical	TRUE	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H	9.8 critical	FALSE	CVSS:3.1/AV:N/AC:L/P	R The depre	CVE-2022-23219	1/14/2022	2 11/8/2022	https://nvd.nist.gCWE-1	20	https://s null	null	
⇔2.26	TRUE	libanl	7.5 high	FALSE	AV:N/ACL/Au:N/C:P/I:P/A:P	9.8 critical	FALSE	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H	9.8 critical	TRUE	CVSS:3.1/AV:N/AC:L/P	R An intege	CVE-2018-6485	2/1/2018	8/24/2020	https://nvd.nist.gCWE-7	87, CWE-190	https://s null	null	
œ2.34	TRUE	libanl	7.5 high	FALSE	AV:N/ACL/Au:N/C:P/I:P/A:P	9.8 critical	TRUE	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H	9.8 critical	FALSE	CVSS:3.1/AV:N/AC:L/P	R The depre	CVE-2022-23218	1/14/2022	2 11/8/2022	https://nvd.nist.gCWE-1	20	https://s null	null	
<2.32.0	TRUE	libani	3.7 low	FALSE	AVIL/ACH/AutN/CP/IIP/AIP	7 high	TRUE	CVSS:3.0/AV:L/AC:H/PR:N/UER/S:U/C:H/EH/A:H	7 high	FALSE	CVSS:3.1/AV:L/AC:H/P	R: A use-aft	CVE-2020-1752	4/30/2020	0 10/28/2022	https://nvd.nist.gCWE-4	16	https://s null	null	
⇔2.26	TRUE	líbani	7.5 high	FALSE	AV:N/ACI_/AU:N/CIP/I:P/AIP	9.8 critical	FALSE	CVS5:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H	9.8 critical	TRUE	CVSS:3.1/AV:N/AC:L/P	R The glob f	CVE-2017-15804	10/22/2017	7 6/20/2018	https://nvd.nist.gCWE-1	19	https://s null	null	
œ2.32	TRUE	libani	7.1 high	FALSE	AV:N/AC:M/Au:N/C:N/I:N/A:C	5.9 medium	TRUE	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	5.9 medium	FALSE	CVSS:3.1/AV:N/AC:H/R	R The Icorv	CVE-2019-25013	1/4/2021	1 11/3/2022	https://nvd.nist.gCWE-1	25	null	null	
<8.44	TRUE	libpcre	5 medium	FALSE	AV:N/ACL/AU:N/C:N/I:N/A:P	5.3 medium	TRUE	CVS5:3.0/AV:N/AC:L/PR:N/UEN/S:U/C:N/EN/A:L	5.3 medium	FALSE	CVSS:3.1/AV:N/AC:L/P	R libpcre in	CVE-2020-14155	6/15/2020	12/3/2022	https://nvd.nist.gCWE-1	90	https://b null	null	
111,11	TRUE	libssl	7.5 high	FALSE	AV:N/ACL/Au:N/C:P/I:P/A:P	9.8 critical	TRUE	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:H/I:H/A:H	9.8 critical	FALSE	CVSS:3.1/AV:N/AC:L/P	R:N/UI:N/S:	CVE-2021-3711	8/24/2021	12/6/2022	https://nvd.nist.gCWE-1	20	null	null	
[1.0.2, 1.0.	TRUE	libssl	4.3 medium	FALSE	AV:N/AC:M/Au:N/C:N/I:N/A:P	5.9 medium	TRUE	CVSS:3.0/AV:N/AC:H/PR:N/UEN/S:U/C:N/E:N/A:H	5.9 medium	FALSE	CVSS:3.1/AV:N/AC:H/R	R:N/UEN/S	CVE-2021-23841	2/16/2021	1/9/2023	https://nvd.nist.gCWE-4	76	null	null	
111,11	TRUE	libssl	5 medium	FALSE	AV:N/ACI_/Au:N/C:P/I:N/A:N	5.3 medium	TRUE	CVS5:3.0/AV:N/AC:L/PR:N/UEN/S:U/C:L/EN/A:N	5.3 medium	FALSE	CVSS:3.1/AV:N/AC:L/P	R OpenSSL:	CVE-2019-1549	9/10/2019	9 10/20/2020	https://nvd.nist.gCWE-3	30	null	null	
[1.0.2, 1.0.	TRUE	libssi	5 medium	FALSE	AV:N/AC:L/Au:N/C:N/I:N/A:P	7.5 high	TRUE	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:N/I:N/A:H	7.5 high	FALSE	CVSS:3.1/AV:N/AC:L/P	R:N/UI:N/S:	CVE-2022-0778	3/15/2022	2 11/9/2022	https://nvd.nist.gCWE-8	35	null	null	
$\rightarrow$	d_	cves	+									:	-				_			

## Figure 95: C3 CVEs (Jarvis)

C D E F G Realiste MDS Realiste Custo	lla info cfila in	do ast file into file name	the info file with	G file info mod timestame	a string	AS.
						-
						(
		ietf-netconf-acm.y				
		sum.exe				
		sum.exe				
a766e1c3bb6449b53c3e368bde18b09a74263aef34083ef46eacc6d38bf857288b1	TRUE	data		2018-05-01700:00:58	10026717@zte.com.cn	
1a85440fe227108470 c79684f692bb2b0 9022f5b939fo4f2a12; a3bf1f143 f5bf7a452	FALSE .exe	idb.exe	/sample_c3.z1p/VSWd2/NVMe/docker/overlay2/62d8H5217b9d2a24045863d59d0a37435880dcd1ddaf84247f06405581252b0/dff/idb.exe	2021-08-25T11:49:52	cancel-streamlocal-forward@o	openssh
1a85440fe227108470 c79684f692bb2b0 9022f5b939fc4f2a12ca3bf1f143 f5bf7a453	TRUE .exe	idb.exe	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/biobs/sha256/b9/b96117f124990405cf9c58558e4b47919f834bdf4ba0e61efd1511dff53129f/data/5	2021-08-25711:49:52	cancel-streamlocal-forward@o	opensst
1a85440fe227108470 c79684f892bb2b0 9022f5b939fc4f2a12; a3bf1f143 f5bf7a452	TRUE .exe	idb.exe	/sample_C3.ztp/VSWd2/WUMe/registry/docker/docker/registry/v2/blobs/sha256/b9/b96117f124990405cf9c88518e4b47919f834bdf4ba0e61efd1511dff53329f/data/F	2021-08-25711:48:52	os@zte.com.cn	
309f67047ae61f9543! 2c612f17a6bd48e f5ccc3995a17a53d58: d4f14be3: 8f7ad5049	TRUE .exe	infcpmp.exe	/sample_C3.stp/VSWd2/NVMe/docker/overlay2/e7db12bca36a50055a802861425ff817b5f8b22c2530x654a8ae87587c000a56/diff/nfc_exe/nfcpmp.exe	2021-08-25T11:46:28	appro@openssl.org	
309f67047ae61f9543f2c612f17a6bd48ef5ccc3995a17a53d58rd4f14be3f8f7ad5049	TRUE .exe	nfcpmp.exe	/sample_C3.zip/VSWd2/Nr/Me/registry/docker/docker/registry//2/biobs/sha256/83/83b31de90563za3ac72b367fb26cx41a1929dd15608662aead0e884c5f333f2/data/	2021-08-25711:46:28	appro@openssl.org	
e51b3a5782e8c41bdt8f5a2ed06f619763dace938c68df7bb0c548bace7c86075d00c	TRUE	0.6 libssh.so.4.8.6	/sample_C3.ttp/V5Wd2/W/We/registry/docker/registry/v2/blobs/sha256/43/4334965acfd86497ce7f7b27b6693789a7f6d13cf6496e733a2eb3bb9b0f0258/data/	2021-08-17703:56:42	auth-agent@openssh.com	
e51b3a5782e8x41bdt8f5a2ed08f619763dace938c68df7bb0x548bace7x86075d00x	TRUE	0.6 libssh.so.4.8.6	/sample_C3.stp/VSWd2/NVMe/registry/docker/docker/registry/v2/biobs/sha256/43/433a965ac1d86497ce777b27b6692789a7f6d13cf6496e733a2eb2b9b0ff0258/data/	2021-08-17703:56:42	hmac-sha1-etm@openssh.com	3
e51b3a5782e8c41bdt 8f9a2ed08f61976 3dace938c68df7bb0x 548bace7: 86075d00x	TRUE	0.6 libsth.so.4.8.6	[sample_C3.ttp]/SWd2/W/We/reentry/docker/registry/v2/biobs/sha256/43/433a983arfd86497co17/7b2766652789a76613c76498e733a2eb3bb9b075238/data/	2021-08-17703:56:42	zlib@coenssh.com	
e51b3a5782e8r41bdt 8f9a2ed08f61976 3dace938c68df7bb0r 548bace7r 86075d00r	TRUE	0.6 libssh.so.4.8.6	/sample_C3.21p/VSWd2/NvWde/registry/docker/docker/docker/setistry/v2/biobs/sha256/43/431a965acfd8449/cer7/b2766912789a76d13cf6496e733a2e62ib/tb0ft028/data/	2021-08-17703:56:42	hmac-md5-etm@openssh.com	
e51b3a5782e8c41bdt 8F9c3ed08H51976 3dace938c68H77bb0c548bace7c86075d01c	FAISE	0.6 libeth to 4.8.6	/sample_C3.jpi/VSW52/NVMMe/doriser/overlau//15hbc65bb2235as6968884stcs8e58x8750db4+bbaeb1ae3b9872053d517esc/ddfilib/libvib.so.4.8.6	2021-08-17003-56-42	statufu@opensih.com	
1865d633x55e5693x23d0ebd99db60d725e3d0597bde5dx2f00622ec0x620bcbd7	TRUE					
1865d633a56e5659c2 3d0eb499db6047 26a340597fdfe5da2f 00622ec0x 620bcbd7	TRUE	ssh-keyscan	/sample_C3.zip/VSWd2/NVMe/docker/overlay2/fc80dafb88f1c%342bd68cdf9160be12c6e2d125e48tfc246d15597e22108a/dff/client.tar/FiLE/usr/bin/ssh-keyscan	2021-01-26T16:36:18		
1865d633a56e5693c2 3d0eb499db6047 26a340597ldfe5da2f 00622ec0c 620bcbd7	TRUE	ssh-keyscan	/sample_C3.zip/VSWd2/NVMe/ssd/hools/client.tar/FILE/usr/bin/ssh-keyscan	2021-01-26716:36:18	umat-64@openssh.com	
1865d633a56e5693c2 3d0eb499db6047 26a340597fdfe5da2f 00622ec0c 620bcbd7	TRUE	ssh-keyscan	/sample_C3.stp/VSWd2/NrMe/registry/docker/docker/egistry/42/biobs/sha256/1f/1fc2519174b4a0ff0aLoe68176e13aa01ff4deb55586725b0962826b052a93/data/F	2021-01-26716:36:18	umac-64@openssh.com	
1865d633a56e5699x2 3d0eb499db6047 26a340597fdfe5da2f 00622ectx 620bcbd7	TRUE	ssh-keyscan	/sample_C3.21p/VSWd2/NVMe/registry/docker/docker/docker/segistry/v2/biobs/sha256/2d/2dx84176d78216f629f00e63184607363ee7922857e916b8810754dc1a791c4/data/	2021-01-26716:36:18	umac-64@openssh.com	
1365d633a56e5693c2 3d0eb499db6047 26a340597fdfe5da2f 00622ec0x 620bcbd7	TRUE	ssh-keyscan	/sample_C3.zip/VSWd2/NVMe/registry/docker/registry/v2/blobs/sha256/95/952863459F9c55434c91e1a31b91463427a3c8873b78a1ca5377ec1dx954c2c/data/F	2021-01-26T16:36:18	umat-64@openssh.com	
1865d633a356c5693c2 3d0eb499db6047 26a340597fdfe5da2f 00622ec0x 620bcbd7	TRUE	ssh-keyscan			umac-64@openssh.com	
1865d633a56e5693c2 3d0eb499db6047 26a340597fdfe5da2f 00622ec0c 620bcbd7	TRUE	ssh-keyscan			umac-64@openssh.com	
1945-6522-55665522-7 2-816-5492-64297 36-2485675676-6-57 01673-e-fr 6306-6-67	-	ech.keveran	Instends (13) (In/VAR42) (In/VAR4		umar.M.Sonarech.com	
		No., IMAG.         Mar., MAG. 24. No., M	Mp. (Mod. 2)         Mp. (Mod. 2)<			ImpubbleImpubbleImpubbleImplementation

## Figure 96: C3 email addresses (Jarvis)

	8	C	D	E	F	JK	L.	M	0	p.	Q
@timestamp	cracked_pw	file_info.SHA3-512	file_info.t	file_info.file_path	file_info.fgi	i homedi	r password	realname	shell	uid	usemame
2023-08-12714:38:46.502500		7b9521ce825ee8aaac3816ac17fc3c	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	1106 ASCII	2 /bin	•	bin	/bin/false		2 bin
2023-08-12T14:38:46.502900		7b9521ce825ee8aaac3816ac17fc3c	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	110b ASCII	8 /var/spi	10 *	mail	/bin/false		8 mail
2023-08-12714:38:46.502900		7b9521ce825ee8aaac3816ac17fc3c	0 shadow	/sample_C3.zip/V5Wd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	110b ASCII	0 /root	*	root	/bin/sh		0 root
2023-08-12714:38:46.502900		7b9521ce825ee8aaac3816ac17fc3c	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	10b ASCII	37 /var	*	Operator	/bin/false		37 operator
2023-08-12714:38:47.065409		95c9l43debf825516dcac0747fb868	e shadow	/sample_C3.zip/VSWd2/TuffDrive/Partition5/ramdisk.bin/FILE/etc/shadow	ASCII	0/	\$5\$\$\$\$kzbWaJ\$07mh0haAf9TW1dKMx22fJGH8h8qTTYgqcgXIMeU016	Linux Administrator	/bin/sh		0 zte
2023-08-12714:38:47.065409		95c9f43debf825516dcar0747fb868	e shadow	/sample_C3.zip/VSWd2/TuffDrive/Partition5/ramdisk.bin/FILE/etc/shadow	ASCII	1 /var/em	p:1	Linux User	/usr/sbin/nologin	1,0	01 sshd
2023-08-12714:38:46.502900		7b9521ce825ee8aaac3816ac17fc3c	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	10b ASCII	65,534 /home	•	nobody	/bin/false	65,5	34 nobody
2023-08-12714:38:47.065409		6e6798329a4e83adc067affbf89f355	St base_wla	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb1791	L1eaHTML	1,111 /home/	ic x	Linux User	/bin/nologin	1,1	11 sctp
2023-08-12714:38:47.085409		95c9143debf825516dcac0747fb868	e shadow	/sample_C3.zip/VSWd2/TuffDrive/Partition4/ramdisk.bin/FILE/etc/shadow	ASCII	0/	\$5\$uFWcf7Dq\$JsJMVVRrNnyVF.p6d705ywegTf24jCezLQNq9KVLsW7	Linux Administrator	/bin/sh		0 admin
2023-08-12714:38:47.085409		95c9f43debf825516dcac0747fb868	e shadow	/sample_C3.zip/VSWd2/TuffDrive/Partition5/ramdisk.bin/FILE/etc/shadow	ASCII	0/	\$5\$uFWcf7Dq\$isJMVVRrNnyVF.p6d709ywegTf24jCezLQNq9KVLsW7	Unux Administrator	/bin/sh		0 admin
2023-08-12714:38:47.085409		95c9f43debf825516dcac0747fb868	e shadow	/sample_C3.zip/VSWd2/TuffDrive/Partition4/ramdisk.bin/FILE/etc/shadow	ASCII	0/	\$5\$SSkzbWaJ\$07mh0haAf9TW1dKMx22fJGH8h8qTTYgqcgXIMei.016	Linux Administrator	/bin/sh		0 zte
2023-08-12714:38:46.502900		7b9521ce825ee8aaac3816ac17fc3d	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	10b ASCII	100 /bin	•	sync	/bin/sync		4 sync
2023-08-12714:38:47.085409	NO PASSWORD	6e6798329a4e83adc067affbf89f355	Stbase_wfa	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb179/	L1eaHTML	1,000 /home/	tte	Linux User,	/bin/sh	1,0	00 zte
2023-08-12714:38:47.085409		95c9f43debf825516dcac0747fb868	e shadow	/sample_C3.zip/VSWd2/TuffDrive/Partition4/ramdisk.bin/FILE/etc/shadow	ASCII	1 /var/err	p1	Linux User	/usr/sbin/nologin	1,0	01 sshd
2023-08-12714:38:45.502900		7b9521ce825ee8aaac3816ac17fc3d	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	100b ASCII	1 /usr/sbi	n *	daemon	/bin/false		1 daemon
2023-08-12714:38:45.502900		7b9521ce825ee8aaac3816ac17fc3c	0 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	10b ASCII	3 /dev		sys	/bin/false		3 sys
2023-08-12714:38:45.502900		7b9521ce825ee8aaac3816ac17fc3d	9 shadow	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/76/76df92	100b ASCII	33 /var/w/	nt*	www-data	/bin/false		33 www-data
	NO PASSWORD	6e6798379a1e83ado167affbf89f39	Uhate wila	/sample_C3.zip/VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb179:	Liez HTML	0 /root		Linux User	/bin/sh		0 root

Figure 97: C3 Password File Analysis (Jarvis)

A II	м			E.	.M	N	AA	AB	AD	AG		AM	AS AT	3	AD :	AV	AW	AX	AY.	- 2A	84	88	BC .	80	8E	17
		. (file_info.file_name	file_info.file_output		thie_info.jfile_					file_info.stat.u			string													
3023-08-1 31103ad158e19b978f7e730ff5ac959b	C55	demo.css	UTF-8 Unicode text		(RegularFil 2023				1,1		103 dabblet.com		http://dabblet.c													
	html	demo_index.html	HTML document text		(RegularFil 2021				1,1		103 www.iconfo	ont.on	https://www.iei				(?manage,	type-my	projects&p	rojectid=1	470028					
2023-08-1.1081da1dc520d06ca452468d87ee013f		bashversion	ELF 64-bit LS8 executab						1,0		to a grouting add		http://gnu.org/l													
2023-08-1 fb81dafdc520d06ca452468d87ea0f3f		bashversion	ELF 64-bit LS8 executab							0	0 www.gnu.or	a l	http://www.gnv													
2023-08-1.d3be096e70bb3baae26c9b36ce115472		ces	ELF 64-bit LSB executab							0	0 curl.ham.se		https://curi.hax	01.54/60	ecs/http-c	cookies.)	steel									
2023-08-1:914e590085e253a71e08362be3f9958b	.50	1004-5.1.50	ELF 64-bit LSB shared of	bjx/sample	(Regularfil 2023	1-08-25711-41/3	5 /sample_c	ofoam/lib	1,1	1,:	101 mmw.lua.or	8	www.lua.org													
2023-08-1 0c5b929813d36bcd8e38ab069b2349b	yin	tetf-netconf-acm.ytn	XML 1.0 document text	t /sample	(RegularFil 2023	-08-05114:39:3	5 /sample (	vswd2/N		0	0 tools.setf.or	8	http://tools.iet/	f.arg/m	g/natcord	d/Egt										
3023-08-1.0c5b929813d36bcd8+38abb69b2348b	yin	ietf-netconf-acm.yin	XML 1.0 document text	t /sample	(RegularFd 2023	-08-05714:39:3	5 /sample (	infoam/sh	1,1		101 trustee.letf.	org	http://trustee.ie													
2023-08-1.2b674dc09649628b04e1a3183db734a2	.svg	ZTELMT.svg	SVG Scalable Vector Gn	teo/sample	(RegularFil 2023	08-25711-44:0	7 /sample (	home/we	1,1	03 1,1	103 www.boher	miancoding.com	http://www.bol	hemion	coding.co	om/sket	th.									
2023-08-1: 6+2f455bfc5cb48d1d1377d85052d429	h	stricheaders.h	C source text C tource,	At/sample	(RegularFil 2023	-08-12102-48:1	# /sample (	VSW//N		0	D ourl.hass.se		https://carl.hao	cs.se/de	DEN/COPYER	ght.htm	á									
2023-08-1.6181das32dbfb2e42547038001bf01c6	h.	tis].h	C source text C source t	tes/sample	(RegularFil 2023	-08-12702:48:1	# /sample of	VSWd2/N		0	0 tools.lett.or	8	https://tools.iet	ef.org/h	itml/draft	t-letf-tis	-11:13-23									
2023-08-1 6181daa32dbfb2e42547038001bf01c6	.b.	tis1.h	C source text C source t	tes/sample	(RegularFil 202)	-08-12702:48:1	9 /sample (	tcfslib/inc		0	0 tools.ietf.or	8	https://tools.iet	ef.org/h	tml/draft	t-letf-tis	-0113-23									
2023-08-1 (Saba5e Je: 7alc64eb6e 784x0757d68e	n.	buffer.h	C source text C source t	tei/sample	(RegularFil 2023	07-16711-15-8	5 /sample (	tcfslib/inc		0	0 www.opens	isl.org	https://www.ee	penssl.c	org/source	e/licens	e.html									
2023-08-1-489c5be65f825998c45d52f98c7903e7	sh	diagnose sh	POSIX shell script text of	ex /sample	(RegularFil 202)	08-25711-41/3	8 /sample 4	V5W/02/N		0	0 izte.com.cm		http://i.zte.com	.cn/N/s	shared/Sol	66657251	x474735a	ad521d710	bf1768/wa	i/osce/d	13026648d2	b41eaa4db4	1101e8338	4e/view?tra	ck id=74	4113621
2023-08-1-c984065c480/0962bc002c30154a5ta0		out	ELF 64-bit LS8 executab	tio / camele	(RegularFil 2021	08.25711.4113	R /sample p	VSWIDD		0	0 nurt have se		https://curl.hax	0.50/12	matteles	of easy	cetost ht	eni.								
2023-08-1 1485680fe227108470e1h5851467Mite	exe	idb.exe	ELF 64-bit LSB executab							0	0 golang.org		https://golang.o													
2023-08-1 1485440fe227108470e1b585146794be	4008	tdb.exe	8LF 64-bit LSB executab							0	D www.gno.o	1	http://www.ats													
3023-08-1 0a31ce97a24345c238655db1430de7bb	SME.	collegse.svr	SVG Scalable Vector Gr							0	0 sketchapp.c		https://sketchad													
2023-08-1.309f67047ae61f954359b118f54702de		nfcpmp.exe	ELF 64-bit LSB executeb							0	0 www.bandu		www.beicku.com													
2023-08-1 [2a2034[/e2E/ed107003attiate2citicite		reemain.exe	ELF 64-bit LSB executab							0	0 developers.		https://develop		ala com	Inextore	Soffarel	Mars/rafe	anna lan/li	and the services	inere-conft	1				
2023-08-1 af8f7df16a69c12fb34f21d6d6cd58b5		de-poreintl.yang	UTF-8 Unicode text, with							0	D www.ste.co		http://www.ste						and a first of							
2023-08-1. +69x9bf12b0x94349x64712f16x2+68d	1-0	arebrant	SLF 64-bit LSB executab							0	0 bredo.me		http://beego.m			Sec. Sec.	and in Factor	Barriel a								
3023-08-1_469a90/12b0e94349ad4712f16x2a46d		webmint	ELF 64-bit LSB executab							0	0 brego.me		http://beego.m													
2023-08-1 #85a11#8110b7b89aa8406d885#5#752	***	dotsfont.e85a11a9130b2b89sa84.ttf							1.1	11	103 mekyle.com		https://mekvie.													
2023-08-1 21e9d2609fbec98115h75e75531rdedc		hangup.svg	SVG Scalable Vector Gr						1.1		IDR sketch.com		https://sketch.c													
2123-08-1 c3197e14de00b1cebfaff0f0502534ed		Kilbyang.so.0.15.346	ELF 64-bit LS8 shared of						1.1		101 www.rtc-ed		http://www.rfc													
2023-08-1 off70302044833cd845105252ea5e0d9		adb	ELF 64-bit LS8 executab							0	0 fst.org		http://fsf.org	-euror.	or District											
2023-08-1, 0017020204453303453002520450005 2023-08-1, 8/9e1384e1365652226456303451002520456005		(mo.h	C source text C source t							0	0 www.opens		http://www.opr													
2023-06-1_009012490000222890010505001111748		unicodedata.cpython-36m-x86_64-16								0	0 ftp.unicode		ftp://ftp.unicod		4											
2023-08-1:0790ara080173eanctosabe810677c34 2023-08-1:00a97480c3957b04680b84a972d4c90c	50	unicodedata.cpython-sem-kee_e4-n								0	0 mp.cr/scode			se.org												
2023-08-1, 204/97/4800 395 7004880 0544/97 7040900 2023-08-1, 204/94/5014-3eboddce 77%607bfd21d5a		PMagene	ELF 64-bit LSB executab UTF-S Unicode text, with							0	0 wiki_tie.com		www.lua.org http://wki.zte.r					distant.	100							
2023-06-1_200294551245400000047790707022054										0	D arts2, rte.com		http://artsr.ite				.action i pa	fiero-out	50000							
	. 675	build_image.sh	POSIX shell script text of							0																
2023-08-1 +058652253ed4358f85cfa3813143c223		pbeig-2	ELF 64-bit LSB executab							0			http://jwvornika				1									
2023-08-1.de53c1685443bt01b5090e44b71c110c		14.5652435036F056579c68.js	ASCI text, with very lo						1,1	03 3,3			g http://schemas.													
2023-08-1 de53c3645443b601b5090e44b71c110r		14.56b243b036f056b79e58.jt	ASCII text, with very los							0			g http://schemas.										(/schemas	-operxenition	ermats.org	@/peck
2023-08-1.de53c3645443b601b5090e44b73c130c		14.56b243b0367056b79o58.js	ASCII text, with very lo						1,3				g http://schemas.									r				
2023-08-1 de53c1645443b601b5090e44b71r110c		14.56b243b0367056b79o58.js	ASCII text, with very lo							0			g http://schemas.													
2023-08-1.de53c1645443b601b5090e44b71c110c		14.56b243b0387059b79o58.js	ASCII text, with very lo						1,1				g http://schemas.													
2023-08-1.de53c1645443b601b5090e44b71c110c		14.56b243b0367056b79c68.js	ASCII text, with very lo						1,1			enxmillormats.og	g http://schemas.	opena	miformats	s.org/of	heeDocum	sent/2006	relationshi	ips/charts	heet*,2e(*(	hartsheet",	null, (xmln	stt.main[0];	"xmins"	with NJ
2023-08-1.de53c1545443b601b5090e44b71c110c		14.56b243b0367056b79o68.js	ASCII text, with very lo							0	0 puri,org															
2023-08-1.91731ee51ac03e8807ea7780a57e2c44		Brdpartylicenses.txt	UTF-8 Unicode text, with							0	0 www.apach		http://www.apa			IS/LICEN!	3E-2.0									
2023-08-1: 62545547e793da068dc580d184cc0e31		opensans.ttf	TrueType Font data, dig						1,1	03 1,3	103 www.varisiy		https://www.xe													
2023-08-1.425455a7w793da0680x580d184cc0w31		opensans.ttf	TrueType Font data, dig							0			http://cscd-2009													
2023-05-1.025v53a7v793da068dx580d184cc0v31	.ttf	opensans.ttf	TrueType Font data, dig						1,1	03 2,3		crt.versagn.com						100								
2023-05-1: 4780/fa0/d33dc3acf61ccd/049abd/06		esel	ELF 64-bit LSB executab							0	D curl.se		https://curl.se/l				pt.html									
2023-08-1:4786Ha0d33dc3acf61cccH049abdf06		curi	SLF 64-bit LSB executab	ble/sample	(RegularFil 2023	-08-26712:28:1	I /sample (	VSWd2/N		0	D curl.se		https://curl.se/v	docs/ss	i-ciphers.)	.html										
2023-08-1-4786ffa0d33dc3acf61cccii049abd106		curl	ELF 64-bit LSB executab	ble/sample	(RegularFil 2023	-08-26712:28:1	\$ /sample (	curl/curl		0	0 example.co	m	https://example	e.com/s	upload.cg	pi .										
2023-08-1-4786#a0d33dc3acf61ccd9049abd906		curi	ELF 64-bit LSB executab	ble/sample	(RegularFil 2023	1-08-26T12:28:1	# /sample (	vswd2/N		0	0 curl.se		https://curl.se/s	docs/ss	(certy, htm	el.										

Figure 98: C3 Infoleak URL Report (Jarvis)

# Sample C3 Finite State Platform Scan Report Excerpts

в > [т	EST V		Download ~
view	Bill of Materials Findings S	Scans Files	
	Risk		Details
	<b>100</b> / 100 0 10 35	65 100	Operating Systems Linux Kernel 4.19.31, Linux Kernel 4.9.115, Linux Kernel 4.19.82 and Linux Kernel 4.4.157
	Findings Detected		FreeRTOS 8.2.3 and FreeRTOS 7.0.0      VxWorks Unknown      Architectures
	Software Components 3,351		- Products Depending On This Artifact August 2023 100
			Created Charles.begian@ngc.com August 30, 2023
	Finding Exploit Intelligence	l₹ Count	Remediation Guidance
	No Known Exploits	43,788 findings	Guidance
	Proof of Concept Exploit	02,049 findings	Address high risk component /VSWd2/NVMe/ssd/1/version /VER/V2.21.01.00B99-2P02-14_20210825191325.sctp
	4 Weaponized	③ 70 findings	/V2.21.01.00B99-2P02-14_20210825191325.sctp/128-11798499 /Izma.uncompressed/sctp@B99-2P02-14.tar
	Reported in the Wild	③ 21 findings	/27877716999d23e036a886aa838f2697bffac22be9e0ec0123£ /layer.tar/ordinaryuserhome/chown
	Exploited By Threat Actors	① 11 findings	Address high risk component /VSWd2/NVMe/docker/overlay2 /2cfa895e679e0723fc1a2dd4bd051eb997e17687fa3e423bd11t /diff/bin/busyboxping

Figure 99: C3 Scan Overview (Finite State Platform)

C3 → TEST ✓ Overview Bill of Materials Findings S	icans	Files					Download V Upload
<ul> <li>Low (10872)</li> <li>Medium (34537)</li> <li>High (460)</li> </ul>	Critical (3	8)		Category No Pro V We Rep	Exploit Intelligence Known Exploits of of Concept Exploit aponized ported in the Wild ploited By Threat Actors		IF Count 43,788 findings ⊙2,049 findings ⊙ 70 findings ⊙ 21 findings ⊙ 11 findings
Ill Filter         Q. Search findings							:
Title		Severity	≕ Risk	Status	CVE	CWE	Found By
CVE-2015-0235 - glibc-devel:2.17	ර	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2015-0235 - glibc:2.17	ම	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2015-0235 - glibc-devel:2.17	ර	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2015-0235 - glibc:2.17	ම	Critical	<b>10</b> /10		CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2016-2108 - OpenSSL:0.9.8za		Critical	<b>9.7</b> /10		CVE-2016-2108	CWE-119	Finite State Monitoring
CVE-2019-3822 - cURL:7.52.1	ଡ	Critical	<b>9.5</b> /10		CVE-2019-3822	CWE-787	Finite State Monitoring
CVE-2019-3822 - cURL:7.55.1	ර	Critical	<b>9.5</b> /10		CVE-2019-3822	CWE-787	Finite State Monitoring

Figure 100: C3 Findings (Finite State Platform)

D	E
category	subcategory
CREDENTIALS	PASSWD_USER_ACCOUNTS
CRYPTO_MATERIAL	PEM_CERTIFICATE_KEY
CRYPTO_MATERIAL	EXPIRED_CERTIFICATE
CRYPTO_MATERIAL	PEM_CERTIFICATE_EXPIRED
SAST_ANALYSIS	USE_AFTER_FREE
SAST_ANALYSIS	HEAP_BUFFER_OVERFLOW
SAST_ANALYSIS	DOUBLE_FREE
CONFIG_ISSUES	SSH_PERMIT_ROOT
SAST_ANALYSIS	UNCHECKED_RETURN_VALUE
CONFIG_ISSUES	SSH_MAX_RETRIES
SAST_ANALYSIS	EXPRESSION_ALWAYS_TRUE
SAST_ANALYSIS	INHERENTLY_DANGEROUS_FUNCTION
SAST_ANALYSIS	IMPROPER_LENGTH_HANDLING
SAST_ANALYSIS	INCORRECT_BEHAVIOR_ORDER
SAST_ANALYSIS	VERY_HIGH_CODE_COMPLEXITY
SAST_ANALYSIS	HIGH_CODE_COMPLEXITY
CREDENTIALS	SHADOW_HARD_CODED_PASSWORDS
CREDENTIALS	PASSWD_HARD_CODED_PASSWORDS
CRYPTO_MATERIAL	SSH_PRIVATE_KEY
CONFIG_ISSUES	SELINUX_DISABLED
CRYPTO_MATERIAL	SELF_SIGNED_CERT
SAST_ANALYSIS	VXWORKS_EXE_NO_PASSWORD
SAST_ANALYSIS	STACK_BUFFER_OVERFLOW
CRYPTO_MATERIAL	PKCS8_PRIVATE_KEY
CVE	KNOWN_VULNERABILITIES
> <u>C3_TEST.</u>	findings +

Figure 101: C3 Findings Categories (Finite State Platform)

A	В	С	D	G	Н	
vulnIdFromTool			cvssVectorString	affectedComponents	exploitCount	maxExploitMaturit
CVE-2020-1967	7.2		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N		2	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I OpenSSL:1.1.1d	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I OpenSSL:1.1.1	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I OpenSSL:1.1.1	1	poc
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I OpenSSL:1.0.2g	1	рос
CVE-2016-8610	7.3	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N	/I OpenSSL:1.0.2g	1	рос
CVE-2018-20843	7.4	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N	/lexpat:2.2.6	1	poc
CVE-2022-25236	8.7	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I expat:2.2.6	1	poc
CVE-2022-25315	7.3		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H			poc
CVE-2019-3822	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H			poc
CVE-2019-5436	7.3		CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/			рос
CVE-2022-1292	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H			рос
CVE-2016-6304	7.2		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2016-8610	7.2		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2010-3010 CVE-2016-7054	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			poc
CVE-2016-6305	7.2		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			poc
CVE-2017-3730	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2016-7054	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2017-3730	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2016-6305	7.2		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2016-8610	7.3		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2016-6304	7.2	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N	I/I OpenSSL:1.1.0	1	рос
CVE-2021-43527	7.3	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I NSS:3.12.4	1	рос
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I OpenSSL:1.0.2n	1	рос
CVE-2022-0435	7.2	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H,	l: Linux Kernel:4.19.82	2	рос
CVE-2018-16601	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H	I/ FreeRTOS:7.0.0	1	poc
CVE-2018-16525	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H	I/ FreeRTOS:7.0.0	1	рос
CVE-2018-16526	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H	I/ FreeRTOS:7.0.0	1	рос
CVE-2018-16526	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H	I/ FreeRTOS:8.2.3	1	poc
CVE-2018-16601	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H	/ FreeRTOS:8.2.3	1	poc
CVE-2018-16525	7.3		CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H			poc
CVE-2019-6974	7.4		CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H			poc
CVE-2020-14305			CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H			poc
CVE-2022-0435	7.2		CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H			рос
CVE-2019-11477			CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2019-11477			CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2019-11475 CVE-2019-11478			CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N			рос
CVE-2015-11478 CVE-2015-8779	8.6		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H			poc
CVE-2013-8779 CVE-2014-9984	8.5					•
			CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H	-		poc
CVE-2014-9761	8.7		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H	-		poc
CVE-2015-7547	8.1		CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H			weaponized
CVE-2015-8778	8.4	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H	-		рос
CVE-2014-9402	7.4			glibc:2.18		рос
CVE-2014-9402	7.4			glibc:2.18		poc
CVE-2014-9984	8.5		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H			рос
CVE-2014-9761	8.7		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H		2	рос
CVE-2015-8778	8.4	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I glibc:2.18	1	рос
CVE-2015-7547	8.1	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H	I/ glibc:2.18	18	weaponized
CVE-2015-8779	8.6	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I glibc:2.18	1	рос
CVE-2022-1292	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H	/I OpenSSL:1.0.2k	1	рос
CVF_2019_11/77	75		CVSS-2 1/AV-N/AC-L/DR-N/LII-N/S-LI/C-N			noc

Figure 102: C3 CVE Exploitability (Finite State Platform)

# **APPENDIX F: CST SCAN REPORT EXCERPTS FOR SAMPLE C4**

Black Duck Binary Analysis Search	and jump to group	🕹 Upload	-	? •	은 charles.begian +
Analysis settings File content					
General					
Name	sample_C4.zip 🖻				
Description	No description given 🗹				
Version	No version given 🗹				
Uploaded	2023-08-10 11:16 (4 days ago) by charles.begian				
Last scanned	2023-08-10 11:27 (4 days ago)				
BDBA engine version used for scanning	20230608				
BDBA frontend version used for calculation	20230615 LATEST				
Protect from data retention					
Notify on new vulnerabilities					
Ether and the state					
File properties					
File	▲ Replace				
File available	No				
SHA1	048a50e0a4c6beeeea42bcdd367ed52eccbc63e4				
Size	312.56 MB (original) / 1.28 GB (scanned)				
Analysis © Remove					
Application type	Linux kernel				
Duration	10 minutes				
Throughput ①	38.96 MB/s				
BDSA database version ①	2023-08-14T11:59:50 STALE				
NVD database version ①	2023-08-14T06:15:00 STALE				
Component database version ③	2023-08-14T04:04:31				
Native fingerprint version	2023-05-31T10:04:47				
Cocoapods fingerprint version	2023-06-07T07:52:47.754010				
Golang fingerprint version	2023-06-08T07:16:22.448950				
Python fingerprint version	2023-06-12T01:47:49.220082				
Low risk tolerance mode	No O				
Include historical vulnerabilities	Yes ©				
CVSS v3 missing score fallback	No @				
E: ~	ure 103: C4 Scan Overview (Black Duck)				

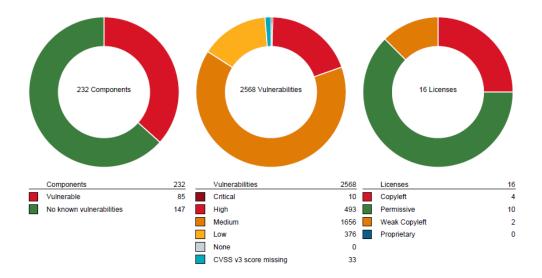
# Sample C4 Black Duck Scan Report Excerpts

Figure 103: C4 Scan Overview (Black Duck)

Report generated 2023-08-13T23:37:57Z https://protecode-sc.com/products/24698759

# sample\_C4.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY



*Figure 104: C4 Scan found 2568 Vulnerabilities (Black Duck)* 

1.1	<b>•</b>	<b>O</b> 1	
1.1	-	all	5

Google cloud keys:

Facebook access tokens:

048a50e0a4c6beeeea42bcdd367ed52eccbc63e4 312.56 MB
523
0
0
2384
0
0
2148
0
38
0
10
4
3238
0

Figure 105: C4 Scan Overview (Black Duck)

0 0

	Α	В	С	D	E	F	G	Н	I.	J	K
1	Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File
2	RSA	409	5 DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-16821-9438040.gz', 'cpu_cur.swv-16821-9438040']
3											
	$\langle \rangle$	C4	nfoleak-a	symmetric	-private	+					: •



leorithm	Bits Format		Encrypted		User			V Attributes	File
SA	4096 PEM	FALSE		BEGIN PUBLIC KEY				["countryName": "BM", "organizationName": "Quolvadis Limited", "commonName": "Quolvadis Root CA 2 G3")	['sample_C4.zip', 'eUS8/DR3/luban/lubanmaster', 'certifi/cacert.per
A	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY				["countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimore CyberTrust Root")	['sample_C4.zip', 'eUS8/DR3/luban/lubanmaster', 'certifi/cacert.per
A	2048 PEM	FALSE	FALSE	BEGIN PUBLIC KEY		2037-12-0	TRUE	["countryName": "US", "organizationName": "VeriSign, Inc.", "organizationalUnitName": "(c) 2008 VeriSign, Inc For authorized use only", "commonName": "VeriSign Universal Root Certification Authority"	['sample_C4.zip', 'eUS8/DR3/luban/lubanmaster', 'certifi/cacert.per
					U V 13 13 13 13 13 13 13 13 13 14 14 14 14 14 14 14 14 14 14 14 14 14				
		FALSE		END PUBLIC KEY				["countryName": "68", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COMCOD CA Limited", "commonName": "COMCOD Certification Authority"]	['sample_C4.zip', 'eUS8/DR3/luban/lubanmaster', 'certifi/cacert.pe

# Figure 107: C4 Symmetric keys (Black Duck)

A	File	Domain
freebsd-isp@freebsd.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/data/msg_32.txt']	freebsd.org
seward@bzip.org	['sample_C4.zip', 'eUSB/DR3/BIN/ccm_cur.swv', 'ccm_cur.swv-128-11043889.lzma', 'lubanmaster', 'libbz2.so.1.0']	bzip.org
dm-devel@redhat.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-16821-9438040.gz', 'cpu_cur.swv-16821-9438040']	redhat.com
inux-serial@vger.kernel.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-16821-9438040.gz', 'cpu_cur.swv-16821-9438040']	kernel.org
seward@bzip.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'boot/kdump.cpio.gz', 'usr/bin/makedumpfile']	bzip.org
posix-rename@openssh.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'lib/libsftp.so']	openssh.com
passwd@ldap.frontec.se	['sample_C4.zip', 'eUSB/DR3/BIN/cp_ cur.swv', 'cpu cur.swv-9605512-128814240.lzma', 'sbin/curl']	frontec.se
seward@bzip.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/iotop', 'libbz2.so.1.0']	bzip.org
seward@bzip.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/lubanctl', 'libbz2.so.1.0']	bzip.org
seward@bzip.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/lubanslave', 'libbz2.so.1.0']	bzip.org
asse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/lzmadec']	tukaani.org
asse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/lzmainfo']	tukaani.org
sh-ed25519-cert-v01@openssh.com	['sample_c4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/ssh-keygen']	openssh.com
cdsa-sha2-nistp384-cert-v01@openssh.com	['sample_cxtp', 'eUSB/DR3/BIN/cpu cur.swv', 'cpu cur.swv-9605512-128814240.lzma', 'usr/bin/ssh-keygen']	openssh.com
asse.collin@tukaani.org	[sample_C4.zip,'eV3B/br/shlvcpu_cur.swv', cpu_cur.swv-9605512-128814240.lzma', usr/bin/sstreegen ]	tukaani.org
asse.collin@tukaani.org	[sample_c4.zip], e03b/bh3/bit/cpu_cdr.sw/, cpu_cdr.sw/9605512-128814240.izma, usr/bin/xzdec] ['sample_c4.zip', eUSB/DR3/BIN/cpu_cdr.sw/, 'cpu_cdr.sw/9605512-128814240.izma', 'usr/bin/xzdec]	tukaani.org
asse.collin@tukaani.org		•
	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/xzgrep'] ['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/c+t/6.2.0/x86_64-pc-linux-gnu/bits/c+tlocale.h']	tukaani.org redhat.com
koz@redhat.com		
koz@redhat.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/c++/6.2.0/x86_64-pc-linux-gnu/bits/messages_members.h']	redhat.com
koz@redhat.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/c++/6.2.0/x86_64-pc-linux-gnu/bits/time_members.h']	redhat.com
ephen@networkplumber.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/include/json_writer.h']	networkplumber
ri@mellanox.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/include/linux/devlink.h']	mellanox.com
uytenh@gnu.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/include/linux/if_bridge.h']	gnu.org
sd@queasysnail.net	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/include/linux/if_macsec.h']	queasysnail.net
priikone@poseidon.pspt.fi	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/include/linux/netdevice.h']	pspt.fi
seward@bzip.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/libbz2.so.1.0.6']	bzip.org
teven.bethard@gmail.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/argparse.py']	gmail.com
w@iki.fi	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/getopt.py']	iki.fi
mauryfa@gmail.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/io.py']	gmail.com
olipsis@pitrou.net	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/io.py']	pitrou.net
nfo@egenix.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/platform.py']	egenix.com
omebody@here.my.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/smtplib.py']	my.org
arek@ziade.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/distutils/tests/test_register.py']	ziade.org
oo@bar.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/test_email.py']	bar.com
cr@socal-raves.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/test_email.py']	socal-raves.org
po@bar.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/test_email_renamed.py']	bar.com
cr@socal-raves.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/test_email_renamed.py']	socal-raves.org
cr@socal-raves.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/data/msg_16.txt']	socal-raves.org
GK500B01D0B8Y@cougar.noc.ucla.edu	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/email/test/data/msg_16.txt']	ucla.edu
V.P.A.Ligtenberg@tue.nl	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/site-packages/networkx/generators/directed.py']	tue.nl
lejandro.weinstein@gmail.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/site-packages/networkx/linalg/laplacianmatrix.py']	gmail.com
/.p.a.ligtenberg@tue.nl	['sample C4.zip', 'eUSB/DR3/BIN/cpu cur.swv', 'cpu cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/site-packages/networkx/readwrite/p2g.py']	tue.nl
erfinion@gentoo.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/site-packages/sepolicy/ init .py']	gentoo.org
hallisey@redhat.com	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/site-packages/sepolicy/gui.py']	redhat.com
ordi@gnu.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/share/i18n/locales/an ES']	gnu.org

Figure 108: Infoleak email addresses (Black Duck)

	IP	IPv6	File
	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
	20.2.20.5	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_520_5_10.80.100.96.xml']
	10.80.100.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_520_5_10.80.100.96.xml']
	10.80.100.201	FALSE	[sample_C4.zip', eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
	10.80.100.201		
		FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
	10.81.1.4	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
	10.11.92.242	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/yang/action-simload.yang']
	10.11.92.242	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/yin/yin.tar.gz', 'action-simload.yin']
)	1.3.2.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/upgrade/3.1.60-to-3.1.61.xml']
	1.3.2.2	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/upgrade/3.1.60-to-3.1.61.xml']
	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/brs-rules.xml']
	0000:0000:0000:0000:0000:0000:00001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0209.lua
ŀ	0000:0000:0000:0000:0000:0000:00001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0213.lua
	0000:0000:0000:0000:0000:0000:00001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0600.lua
5	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0601.lua
	0000:0000:0000:0000:0000:0000:0000:0001	TRUE	['sample_c4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0711.lua
1	0000:0000:0000:0000:0000:0000:0000:0001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0807.lua
1	0000:0000:0000:0000:0000:0000:0000:0001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0905.lua
)	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0915.lua
	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1117.lua
	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1317.lua
	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1605.lua
	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1707.lua
	0000:0000:0000:0000:0000:0000:0000:0001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1708.lua
5	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1808.lua
•	0000:0000:0000:0000:0000:0000:0000:0001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1809.lua
3	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1907.lua
, )	0000:0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1908.lua
,	0000:0000:0000:0000:0000:0000:0000:0001	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-2005.lua
, 	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_cneck/lua/CC-TransportNetwork-brs-2003.lua
,	0000:0000:0000:0000:0000:0000:0000:0001		
5		TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-2206.lua
	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-2703.lua
1	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-2915.lua
5	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-3901.lua
	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-4100.lua
	0000:0000:0000:0000:0000:0000:0000	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-4610.lua
	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
	10.0.0.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
	10.1.1.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
	10.2.2.2	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
	2011:0db8:85a3:0000:1319:8a2e:0370:7366	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
	2011:0db8:85a3:0000:1319:8a2e:0370:7366	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/action-modiagnose-getaclrulestatdtm.yang']
	10.2.2.4	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/action-modiagnose-ippingdtm.yang']
	10.2.2.3	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/action-modiagnose-ippingdtm.yang']
	2011:0db8:85a3:0000:1319:8a2e:0370:7366	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/action-modiagnose-ippingdtm.yang']

## Figure 109: C4 Infoleak IP addresses (Black Duck)

A	B	c
1 Address	Vendor	File
2 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUS8/DR3/BIN/ccm_cur.swv', 'ccm_cur.swv-128-11043889.lzma', 'init_c.tar', '9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/layer.tar', 'etc/network/interfaces']
3 00:00:00:FF:FF:FF	Officially Xerox	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/iotop', 'libpython2.7.so.1.0']
4 00:00:00:FF:FF:FF	Officially Xerox	['sample_C4.zip', 'eUS8/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/lubanctl', 'libpython3.7m.so.1.0']
5 00:00:00:FF:FF:FF	Officially Xerox	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/lubanslave', 'libpython3.7m.so.1.0']
6 f4:6d:04:47:2f:ae	ASUSTek COMPUTER INC.	['sample_C4.zip', 'eUS8/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/lib/python2.7/site-packages/IPy.py']
7 00:00:00:FF:FF:FF	Officially Xerox	['sample_C4.zip', 'eUS8/DR3/BIN/ccm_cur.swv', 'ccm_cur.swv-128-11043889.Izma', 'lubanmaster', 'libpython3.7m.so.1.0']
8 00:11:22:33:44:55	CIMSYS Inc	[sample_C4.zip', 'eUSB/DR3/BIN/registry_cur.swv', 'registry_cur.swv', 'registry_cur.swv', 'registry_tar', '539:395560717880d9afa658caeb8c3efcf33256e34b336917d8603f2806e045/layer.tar', 'etc.nommu/network/interfaces']
9 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR3/BIN/registry_cur.swv', 'registry_cur.swv-128-4842459.lzma', 'registry.tar', '539c396560717880d9afa658caeb8c3efcf33256e34b336917d8603f2806e045/layer.tar', 'etc/network/interfaces']
10 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR3/luban/linit_c.tar', 'bdf239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/layer.tar', 'etc/network/interfaces']
11 44:33:4C:06:06:ee	Shenzhen Bilian electronic CO.,LTD	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
12 00:00:00:FF:FF:FF	Officially Xerox	['sample_C4.zip', 'eUS8/DR3/luban/lubanmaster', 'libpython3.7m.so.1.0']
13 44:33:4C:06:06:ee	Shenzhen Bilian electronic CO.,LTD	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'boot.out']
14 00:11:22:00:11:22	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'boot.out']
15 00:a0:c9:00:00:02	Intel	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
16 00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'boot.out']
17 00:11:22:cc:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'boot.out']
18 00:11:22:00:00:22	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'boot.out']
19 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'boot.out']
20 00:11:22:00:11:22	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
21 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'etc.nommu/network/interfaces']
22 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUS8/DR4/ramdisk.bin', 'etc/network/interfaces']
23 44:33:4C:06:06:ee	Shenzhen Bilian electronic CO.,LTD	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'boot.out']
24 00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
25 00:11:22:00:11:22	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'boot.out']
26 00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'boot.out']
27 00:11:22:cc:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'boot.out']
28 00:11:22:cc:44:55	CIMSYS Inc	['sample_C4.zip', 'eUS8/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
29 00:11:22:00:00:22	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'boot.out']
30 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'boot.out']
31 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'etc.nommu/network/interfaces']
32 00:a0:c9:00:00:00	Intel	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
33 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUS8/DR5/ramdisk.bin', 'etc/network/interfaces']
34 00:11:22:00:00:22	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
35 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'HWM.EXE']
36 00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'vm_deploy,json']
37 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUS8/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'boot/kdump.cpio.gz', 'etc/network/interfaces']
38 00:11:22:33:44:55	CIMSYS Inc	['sample_c4.zip', 'eUS8/DR3/8IN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.Izma', 'etc.nommu/network/interfaces']
39 00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUS8/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'etc/network/interfaces']
< > C4	infoleak-macs +	
Pres de		

Figure 110: C4 Infoleak MAC addresses (Black Duck)

A	В	С	D	E	F
1 Password	User	Algorithm	Salted	Hashed	File
2	root		FALSE	FALSE	['sample_C4.zip', 'eUS8/DR3/8IN/ccm_cur.swv', 'ccm_cur.swv', 'ccm_cur.swv', 'lcm_cur.swv', 'init_c_tar', '9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/layer.tar', 'etc/passwd']
3 vY17tW3kiRIADnks0lgyJ0	root	MD5	TRUE	TRUE	['sample_C4.zip', 'eUS8/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'boot/kdump.cpio.gz', 'etc/passwd']
4 07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXIMeL016	zte	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'etc/shadow']
5 JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUS8/DR3/8IN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.Izma', 'etc/shadow']
6	root		FALSE		['sample_C4.zip', 'eUS8/DR3/BIN/registry_cur.swv', 'registry_cur.swv-128-4842459.lzma', 'registry_tar', '539c396560717880d9afa658caeb8c3efcf33256e34b336917d8603f2806e045/layer.tar', 'etc/passwd']
7	root		FALSE	FALSE	['sample_C4.zip', 'eUS8/DR3/luban/init_ctar', '9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/layer.tar', 'etc/passwd']
8 07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXIMeL016	zte	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUS8/DR4/ramdisk.bin', 'etc/shadow']
9 JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUS8/DR4/ramdisk.bin', 'etc/shadow']
10 07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXIMeL016	zte	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUS8/DR5/ramdisk.bin', 'etc/shadow']
11 JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUS8/DR5/ramdisk.bin', 'etc/shadow']
12					
< > C4 infoleak-passwords +					I 4



A	8	C
Url	File	Domain
http://www.w3.org/2001/XMLSchema-instance	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/bcs-rules.xml']	w3.org
https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/CSL/NRCSL/nr_cc_bcs_data.lua']	github.con
https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/CSL/NRCSL/nr_cc_bcs_public.lua']	github.com
https://docs.oracle.com/javase/8/docs/api/java/util/stream/package-summary.html#package.description	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/DSL/NRDSL/collection.lua']	oracle.com
https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/lua/CC-Radio-bcs-10090.lua']	github.con
https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/lua/CC-Radio-bcs-10093.lua']	github.con
https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/lua/CC-Radio-bcs-10094.lua']	github.com
http://www.wl.org/2001/J0MLSchema	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/xml_rule/cons.xsd']	w3.org
sftp://username@10.11.92.242:21/simload/T35 64antBCweight 20180404 ServiceBeam32.dat	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/vang/action-simload.vang']	Unknown
sftp://username@10.11.92_242:21/simload/T35_64antBCweight_20180404_ServiceBeam32.dat	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/yin/yin.tar.gz', 'action-simload.yin']	Unknown
https://docs.oracle.com/javase/8/docs/api/java/util/stream/package-summary.html#package.description	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/upgrade/public/nrmodel/nr upgrade bcs collection.lua"]	oracle.com
sftp://username@10.11.92.242:21/rules.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bsa/bsa/yang/action-internal-smartops.yang']	Unknown
sftp://username@10.11.92.242;21/rules.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bsa/bsa/vin/vin.tar.gz', 'action-internal-smartops.vin']	Unknown
stp://username@10.11.92.42/21/ver/verFile.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yang/action-bum.yang']	Unknown
stp://username@172.0.0.3008/file/JrGain0.txt	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yang/action-bum.yang']	Unknown
stp://pot/min.stp://pome	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yang/action-modiagnose-rru.yang']	Unknown
stp://isername@10.11.52.24221/verfile.tar	['sample_G4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/vin/vin.tar.gz', 'action-bum.vin']	Unknown
Stop/j username@pi2.o.0.3008/file/fiv/sian0.txt	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yin/yin/ar.gz', 'action-bum.yin']	Unknown
sttp://toetmaneguize.com/security/interiment/toamu.com/ sttp://rooffed.scl.113.186/22/home	[sample_C4.zip', eUSB/DR3/1/nfoam/1/model/bum/cm/yin/yin.tar.gz', action-bum.yin'] ['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yin/yin.tar.gz', 'action-modiagnose-rru.yin']	Unknown
sttp://jrongeuoz.iis.ie/z/nome@10.119.242/00/ert/zte.pfx	[sample_C4.zip', eUSB/DR3/1/model/certm/certm/yin/yin.tar.gz, action-modiagnose-rru.yin ] [sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yang/action-certm.yang']	Unknown
		Unknown
stp://username@illoll.is2.242:80/Gert/crosscert.p7b	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yang/action-certm.yang']	Unknown
stp://username@10.11.92.242:80/cert/zte.cer	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yang/action-certm.yang']	
sttp://username@10.11.92.242:80/cert/zte.pfx	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yin/yin.tar.gz', 'action-certm.yin']	Unknown
sftp://username@10.11.92.242:80/cert/crosscert.p7b	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yin/yin.tar.gz', 'action-certm.yin']	Unknown
sftp://username@10.11.92.242:80/cert/zte.cer	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yin/yin.tar.gz', 'action-certm.yin']	Unknown
https://docs.oracle.com/javase/8/docs/api/java/util/stream/package-summary.html#package.description	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/cms/cm/consistency_check/DSL/NRDSL/collection.lua']	oracle.con
sftp://username@10.11.92.242:21/backup/backup_01.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yang/action-BrM.yang']	Unknown
sftp://username@10.11.92.242:21/dv/MEId_AppRadioMode.cpu	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yang/action-DvFunction.yang']	Unknown
sftp://username@10.11.92.242:21/dv/dvupdate.cpu	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yang/action-DvFunction.yang']	Unknown
sftp://root@10.62.113.186:22/home/1_2_eNB-pmrule_ITBBU.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yang/action-NeFileBr.yang']	Unknown
sftp://username@10.11.92.242:21/backup/backup_01.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yin/yin.tar.gz', 'action-BrM.yin']	Unknown
sftp://username@10.11.92.242:21/dv/MEId_AppRadioMode.cpu	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yin/yin.tar.gz', 'action-DvFunction.yin']	Unknown
sftp://username@10.11.92.242:21/dv/dvupdate.cpu	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yin/yin.tar.gz', 'action-DvFunction.yin']	Unknown
sftp://root@10.62.113.186:22/home/1_2_eN8-pmrule_IT88U.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/brm/yin/yin.tar.gz', 'action-NeFileBr.yin']	Unknown
sftp://username@10.11.92.242:21/fm/UserDefineAlminfo.json	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/fm/yang/action-fm.yang']	Unknown
sftp://username@10.11.92.242:21/fm/UserDefineAlminfo.json	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/common/fm/yin/yin.tar.gz', 'action-fm.yin']	Unknown
https://docs.oracle.com/javase/8/docs/api/java/util/stream/package-summary.html#package.description	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dcs/cm/consistency_check/DSL/NRDSL/collection.lua']	oracle.com
http://www.zte.com.cn	['sample_C4.zip', 'eU58/DR3/1/nfoam/1/model/dvbum/dv/vang/dv-equipment.vang']	com.cn
http://www.zte.com.cn	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvbum/dv/yang/dv-noreinit.yang']	com.cn
http://www.ate.com.cn	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvcommon/dv/vang/dv-function.vang']	com.cn
http://www.w3.org/2001/X0MLSchema-instance	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvite/dv/consistency_check/DV-rules.xml']	w3.org
http://www.baidu.com/link?url=n9222QR078C978kjHr/WjeWhQA25T0XBKBcSPyM554jF9Yro1P8YoCrghsv9EGSfT7glhfcd2HvpyIRlinWUjyQDMYbXrqcHktINBdMiqlgjuh58j9hFknCzaChi23W	['sample_Chize', 'eUSB/DR3/1/nfoam/1/model/dvite/dv/vang/dv-ite.vang']	baidu.com
http://www.baidu.com/link?url=q6Ddq0GmgEDeVP-YgbUumWY37Builix39vCrfOXsCbkmoOm89MgECWU_Oe8VExxP0Nxa7B0pL0N53XL4evsrx2mVErMyADgtBi	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvlte/dv/yang/dv-lte.yang']	baidu.com
nttp://www.aadducdow/inite/titreptodpomicpotery/rygioubines/site/site/site/site/site/site/site/si	[sample_C4.zip', eUSB/DR3/1/nfoam/1/model/dvite/dv/vinty.ng/dv/ret.yang] ['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvite/dv/vinty.ntar.gz', 'dv-Ite.vin']	baidu.com
http://www.aedu.com/inter/unitedz2dato/tecs/najming/emig/emig/asto/tecs/pass/granulasto/casted/pass/granula	[sample_C4.zip', eUSB/DR3/1/nfoam/1/model/dv/te/dv/yin/yin.tar.gz', dv-ite.yin'] ['sample_C4.zip', eUSB/DR3/1/nfoam/1/model/dv/te/dv/yin/yin.tar.gz', 'dv-ite.yin']	baidu.com
undh/) www.wander.com/uniter.com/de	[ sample_c4.zip , ecos) uks/ 1/moan/ 1/model/ ovice/ ov/ ym/ ym/ ar.gz , ov-rie-ym ]	uenud.com

Figure 112: C4 Infoleak URLs (Black Duck)

A	8	C	D	E	, F	G	Н	1		K	L	M	N
	e Version	Latest version		Matching type 0	CVSS		Object compilation date			Object SHA1	CVSS3		CVSS vector (v3)
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match		10 2014-09-28T19:55:00Z		bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s			0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match		10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash		79151d52932639	6	0 AV:N/AC:L/Au:N:/C:C/I:C/A:0	
bash	4.2.50	5.2.15	CVE-2014-7187	Exact match		10 2014-09-28T19:55:00Z	2019-02-21T10:51:53Z	bash		79151d52932639		0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match		10 2014-09-28T19:55:00Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af21435	de .	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match		10 2014-09-28719:55:002	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d52932639	5	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7186	Exact match		10 2014-09-28T19:55:00Z	2019-02-21710:51:532	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d52932639	5	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match		10 2014-09-25T01:55:00Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af21435	di .	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match		10 2014-09-25T01:55:002	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d52932639	5	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-7169	Exact match		10 2014-09-25T01:55:00Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d52932639	5	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match		10 2014-09-30T10:55:00Z	2021-01-26T16:32:01Z	bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s	3712a04af21435	di l	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match		10 2014-09-30T10:55:00Z	2019-02-21710:51:532	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d52932639	5	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-6278	Exact match		10 2014-09-30710:55:002	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d52932639	6	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match		10 2014-09-27722:55:002	2021-01-26T16:32:01Z	bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s	3712a04af21435	di l	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match		10 2014-09-27722:55:002	2019-02-21T10:51:53Z	bash	sample C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d52932639	6	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2014-6277	Exact match		10 2014-09-27722:55:002	2019-02-21T10:51:53Z	bash	sample C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d52932639	5	0 AV:N/AC:L/Au:N:/C:C/I:C/A:	
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match		5.9 2017-09-13T08:53:252	2021-01-26T16:32:01Z	bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s	3712a04af21435	6	7.5	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match		5.9 2017-09-13108:53:257	2019-02-21710:51:537	hash		79151d52932639		7.5	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O
bash	4.2.50	5.2.15	CVE-2016-7543	Exact match		5.9 2017-09-13T08:53:252	2019-02-21710:51:537	bash		79151d52932639		7.5	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O
bash	4.2.50	5.2.15	CVE-2019-18276	Exact match		3.8 2019-11-29T14:52:13Z		bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s			7.8	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:C
bash	4.2.50	5.2.15	CVE-2019-18276	Exact match		3.8 2019-11-29T14:52:13Z	2019-02-21T10-51:537	bash		79151d52932639		7.8	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:C
bash	4.2.50	5.2.15	CVE-2019-18276	Exact match		3.8 2019-11-29714:52:132		hash		79151d52932639		7.8	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:C
bash	4.2.50	5.2.15	CVE-2016-0634	Exact match		3.8 2017-08-24T16:24:21Z		bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s			5.2	AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/
bash	4.2.50	5.2.15	CVE-2016-0634	Exact match		3.8 2017-08-24T16:24:21Z		hash		79151d52932639		5.2	AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/
bash	4.2.50	5.2.15	CVE-2016-0634	Exact match		3.8 2017-08-24716:24:212		bash		79151d52932639		5.2	AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RI:O.
bash	4.2.50	5.2.15	CVE-2019-9924	Exact match		3.6 2019-03-22T15:28:31Z		bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s			7.6	AV:L/AC:L/PR:N/UI:N/5:U/C:H/I:H/A:H/E:P/RL:C
bash	4.2.50	5.2.15	CVE-2019-9924	Exact match		3.6 2019-03-22715:28:312		bash		79151d52932639		7.6	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:C
bash	4.2.50	5.2.15	CVE-2019-9924	Exact match		3.6 2019-03-22715:28:312		bash		79151d52932639		7.6	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:C
bash	4.2.50	5.2.15	CVE-2022-3715	Exact match		3 2023-01-06T12:22:07Z		bash	sample C4.zip:eUSB/DR3/BIN/cpu cur.swv:cpu cur.s			5.1	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:P/RL:W/
bash	4.2.50	5.2.15	CVE-2022-3715	Exact match		3 2023-01-06T12:22:07Z		bash		79151d52932639		5.1	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:P/RL:W/
bash	4.2.50	5.2.15	CVE-2022-3715	Exact match		3 2023-01-06T12:22:07Z		bash		79151d52932639		5.1	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:P/RL:W/
bash	4.2.50	5.2.15	CVE-2016-9401	Exact match		2.1 2017-01-23721:59:002		bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s				Av:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
bash	4.2.50	5.2.15	CVE-2016-9401	Exact match		2.1 2017-01-23721:59:002		bash		79151d52932639			AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
bash	4.2.50	5.2.15	CVE-2016-9401	Exact match		2.1 2017-01-23721:59:002 2.1 2017-01-23721:59:002		bash		79151d52932639			AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
binutils	2.23.52		L1 CVE-2017-7614	Exact match		7.5 2017-04-09T14:59:00Z			sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s				AV:I/ACI/PR:N/U:N/S:U/C:H/I:H/A:H
binutils	2.23.52		1 CVE-2017-7614	Exact match		7.5 2017-04-09T14:59:00Z				1dcd22fdacc1c0			AV:N/ACL/PR:N/UI:N/S:U/C:H/I:H/A:H
binutils	2.23.52		11 CVE-2017-7614	Exact match		7.5 2017-04-09114:59:002				1dcd22fdacc1c0			AV:N/ACI/PR:N/UI:N/S:U/C:H/I:H/A:H
	2.23.52		11 CVE-2014-9939	Exact match									AV:N/ACI/PR:N/UI:N/S:U/C:H/I:H/A:H
binutils	2.23.52			Exact match		7.5 2017-03-21106:59:002			sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	1dcd22fdacc1c0			
binutils			1 CVE-2014-9939			7.5 2017-03-21106:59:002							AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
binutils	2.23.52		1 CVE-2014-9939	Exact match		7.5 2017-03-21T06:59:00Z				1dcd22fdacc1c0			AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
binutils	2.23.52		1 CVE-2014-8504	Exact match		7.5 2014-12-09T23:59:00Z			sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s			0 AV:N/AC:L/Au:N:/C:P/I:P/A:	
binutils	2.23.52		11 CVE-2014-8504	Exact match		7.5 2014-12-09T23:59:00Z				1dcd22fdacc1c0		0 AV:N/AC:L/Au:N:/C:P/I:P/A:	
binutils	2.23.52		11 CVE-2014-8504	Exact match		7.5 2014-12-09T23:59:00Z				1dcd22fdacc1c0		0 AV:N/AC:L/Au:N:/C:P/I:P/A:	
binutils	2.23.52		11 CVE-2014-8503	Exact match		7.5 2014-12-09T23:59:00Z			sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s			0 AV:N/AC:L/Au:N:/C:P/I:P/A:	
binutils	2.23.52		1 CVE-2014-8503	Exact match		7.5 2014-12-09T23:59:00Z				1dcd22fdacc1c0		0 AV:N/AC:L/Au:N:/C:P/I:P/A:	
binutils	2.23.52	2.4	1 CVE-2014-8503	Exact match		7.5 2014-12-09T23:59:002	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR5/ramdisk.bin:zdbagent	1dcd22fdacc1c0	5	0 AV:N/AC:L/Au:N:/C:P/I:P/A:	

Figure 113: C4 CVEs (Black Duck)

Ready

≡ <sup>I</sup> CODESentry <sup>™</sup>		
+ NEW SCAN	N-DAY FINDINGS 0	ZERO-DAY FINDINGS 100
.III Dashboard	Security Score	Score
Summary	57 Artifact 99 Scan Security 99 Quality	100 Artifact 100 Scan Quality
🖭 xDevOps 🔿	5487 Findings 3,000	0 Findings
NG Evaluation	2,000	None Discovered
C A1	0	0 Low Medium High Critical
<b>©</b> A2		
<b>©</b> A3	NG Evaluation > C4 > sample_C4.zip: Scan Done, Scan Dep	th: Shallow

# Sample C4 Code Sentry Scan Report Excerpts

Figure 114: C4 Scan Overview (Code Sentry)

### 

## <sup>I</sup>CODESentry<sup>-</sup>

### **N-Day Findings Summary**

Name	Version	Vendor	Security Score	Number of Vulnerabilities	Path
apimachinery	kubernetes- 1.8.15	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/lpm
apimachinery	kubernetes- 1.8.15	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/lpm_ cur.swv
audit	2.8.5	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
audit	2.8.5	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
azure-sdk-for- go	26.3.0	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/ registry_cur.swv
bash	4.2.53	gnu	2	3	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
bash	4.2.53	gnu	2	3	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
bash	4.2.53	unspecified	0	6	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
bash	4.2.53	unspecified	0	6	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
binutils	gdb_7_6_2- 2013-12-08	unspecified	7	11	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
binutils	gdb_7_6_2- 2013-12-08	unspecified	7	11	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
binutils- arm64-cross	0.11	unspecified	15	1	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
binutils- arm64-cross	0.11	unspecified	15	1	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
binutils-gold	insight_6_6- 20070208	unspecified	2	1	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
binutils-gold	insight_6_6- 20070208	unspecified	2	1	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
busybox	1_31_1	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/ccm_ cur.swv
busybox	1_31_1	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/luban/init_ c.tar/9df239d952c8a53c81a44409d464b26a354fl5c6 743096fl c46e4556c0d44acb/layer.tar/bin/busybox
busybox	1.26.2	busybox	2	16	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/ registry_cur.swv
busybox	1.26.2	busybox	2	16	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
busybox	1.26.2	busybox	2	16	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
cgdb	0.5.1	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin
cgdb	0.5.1	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR5/ ramdisk.bin
client_golang	0.9.0	prometheus	47	1	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/ registry_cur.swv
cobra	1.1.1	unspecified	100	0	NG Evaluation/C4/sample_C4.zip/eUSB/DR3/BIN/ registry_cur.swv
coreutils	8.14	gnu	28	2	NG Evaluation/C4/sample_C4.zip/eUSB/DR4/ ramdisk.bin

www.grammatech.com

Page 2 / 452

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 115: C4 N-day findings (Code Sentry)

<sup>I</sup>CODESentry<sup>-</sup>

## GRAMMATECH

## **N-Day Findings**

Findings for sample\_C4.zip

Scan Depth: Shallow MD5: cb599c8543567aed45b2eb8t715aabce Number of Vulnerabilities: 5487

#### linux\_kernel [linux] 4.19.82

Match Level: High Security Score: 0 Path: NG Evaluation/C4/sample\_C4.zip/eUSB/DR4/ramdisk.bin Component ID: c456942e-8b5f-4cb7-8729-926c128caf95 Score Distribution: I Unassigned: 0 I None: 26 I Low: 267 A Medium: 813 I High: 462 Critical: 35

Severity	Score	CVSS Version	Vulnerability ID	Description
Critical	10	2.0	24041	Linux Kernel rndis.c OID_GEN_SUPPORTED_LIST Memory Corr
Critical	10	2.0	48120	Linux Kernel video4linux (V4L) uvcvideo uvc_driver.c uv
Critical	10	2.0	49957	Linux Kernel libertas Subsystem drivers/net/wireless/li
Critical	10	2.0	51253	Linux Kernel sctp net/sctp/sm_statefuns.c FWD-TSN Chunk
Critical	10	2.0	61788	Linux Kernel drivers/net/e1000e/netdev.c Ethernet Frame
Critical	10	2.0	67243	Linux Kernel fs/nfsd/nfs4xdr.c NFS XDR Compound Request
Critical	10	2.0	67896	Linux Kernel L2TP drivers/net/pppol2tp.c pppol2tp_xmit
Critical	10	2.0	74679	Linux Kernel Bluetooth net/bluetooth/l2cap_core.c l2cap
Critical	10	2.0	93755	Linux Kernel drivers/target/iscsi/iscsi_target_paramete
Critical	10	2.0	104658	Linux Kernel /netfilter/nf_conntrack_proto_dccp.c DCCP
Critical	10	2.0	107650	Linux Kernel hugetlb_entry Callback Handling Unspecifie
Critical	10	2.0	122243	Linux Kernel OZWPAN USB Host Controller Driver ozhcd.c
Critical	10	2.0	122244	Linux Kernel OZWPAN USB Host Controller Driver ozusbsvc
Critical	10	2.0	137359	Linux Kernel drivers/usb/usbip/usbip_common.c usbip_rec
Critical	10	2.0	148130	Linux Kernel nf_ct_frag6_queue() Function IPv6 Packet D
Critical	10	2.0	156288	Linux Kernel drivers/net/macsec.c macsec_start_xmit() F
Critical	10	2.0	179535	Linux Kernel drivers/char/random.c crng_ready() Functio
Critical	9.8	3.0	205886	Linux Kernel sound/soc/codecs/wcd9335.c wcd9335_codec_e
Critical	9.8	3.0	212917	Linux Kernel drivers/net/ethernet/hisilicon/hns3/hns3pf
Critical	9.8	3.0	212918	Linux Kernel drivers/net/wireless/ath/ath6kl/wmi.c ath6
Critical	9.8	3.0	212920	Linux Kernel fs/cifs/smb2pdu.c SMB2_write() Function re
Critical	9.8	3.0	212921	Linux Kernel fs/cifs/smb2pdu.c SMB2_read() Function req
Critical	9.8	3.0	212942	Linux Kernel drivers/net/wireless/rsi/rsi_91x_mac80211
Critical	9.8	3.0	212953	Linux Kernel kernel/trace/trace.c allocate_trace_buffer
Critical	9.8	3.0	218237	Linux Kernel drivers/net/wireless/marvell/mwifiex/sta_i
Critical	9.8	3.0	218239	Linux Kernel drivers/net/wireless/marvell/libertas/cfg
Critical	9.8	3.0	226740	Linux Kernel drivers/input/input.c input_default_setkey

www.grammatech.com

Page 11 / 452

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 116: C4 Vulnerabilities (mapped to CVEs in the report) (Code Sentry)

# GRAMMATECH

# <sup>I</sup>CODESentry<sup>-</sup>

Zero-Day Findings

Findings for sample\_C4.zip

#### Scan Depth: Shallow MD5: cb599c8543567aed45b2eb8f715aabce

### Top 25 CWE Findings

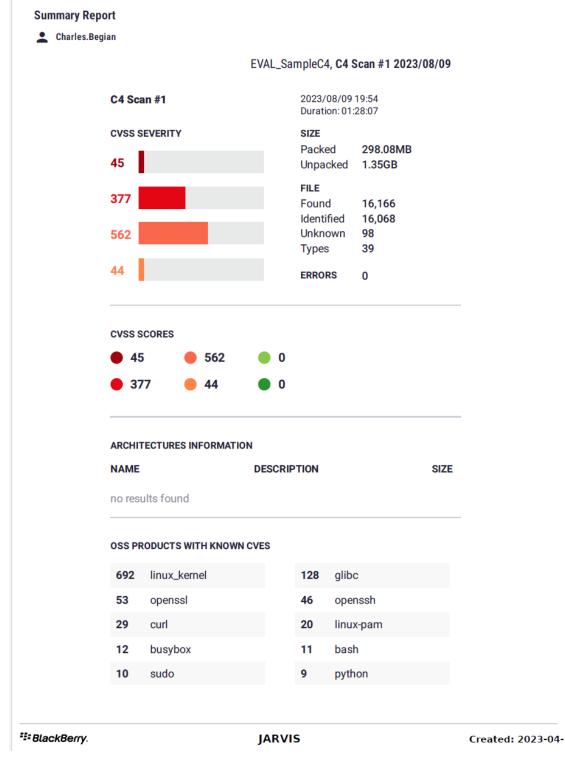
Rank	ID	Name	Instances
1	CWE:787	Out-of-bounds Write	-
2	CWE:79	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	-
3	CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0
4	CWE:20	Improper Input Validation	-
5	CWE:125	Out-of-bounds Read	-
6	CWE:78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0
7	CWE:416	Use After Free	0
8	CWE:22	Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")	-
9	CWE:352	Cross-Site Request Forgery (CSRF)	-
10	CWE:434	Unrestricted Upload of File with Dangerous Type	-
11	CWE:476	NULL Pointer Dereference	-
12	CWE:502	Deserialization of Untrusted Data	-
13	CWE:190	Integer Overflow or Wraparound	-
14	CWE:287	Improper Authentication	-
15	CWE:798	Use of Hard-coded Credentials	0
16	CWE:862	Missing Authorization	-
17	CWE:77	Improper Neutralization of Special Elements used in a Command ("Command Injection")	-
18	CWE:306	Missing Authentication for Critical Function	-
19	CWE:119	Improper Restriction of Operations within the Bounds of a Memory Buffer	0
20	CWE:276	Incorrect Default Permissions	-
21	CWE:918	Server-Side Request Forgery	-
22	CWE:362	Concurrent Execution using Shared Resource with Improper Synchronization ("Race Condition")	-
23	CWE:400	Uncontrolled Resource Consumption	-
24	CWE:611	Improper Restriction of XML External Entity Reference	-
25	CWE:94	Improper Control of Generation of Code ("Code Injection")	-

#### All Other CWE Findings (Excluding Top 25 CWEs)

Severity	Score	CWE ID	Name	Instances

None

Figure 117: C4 Zero-day findings (Code Sentry)



# Sample C4 Jarvis Scan Report Excerpts

Figure 118: C4 Scan Overview (Jarvis)

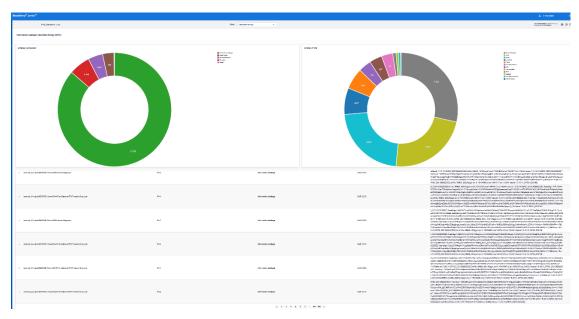


Figure 119: C4 Information leakage (Jarvis)

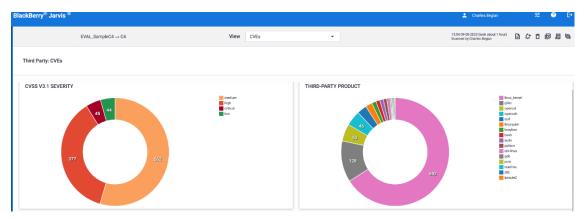


Figure 120: CVSS Severity Report (Jarvis)

ackBerry <sup>®</sup> Jai	rvis <sup>®</sup>										
Scan Results	Charles.Begian@ ▼	EVAL_Sa	mpleC4 🔻								
COMPONENT	\$ NAME	¢ DATE	¢ CRITICAL	¢ HIGH	\$ MEDIUM	¢ LOW	PACKED SIZE	UNPACKED SIZE	IDENTIFIED	<b>≑</b> FOUND	\$ TYPES
EVAL_Sampl	C4	2023/08/09	45	377	562	44	298.08MB	1.35GB	16068	16166	39

## Figure 121: C4 CVE Summary by Severity (Jarvis)

	A	8	C	D	E	F	G	н	J	K	L	М	N	0	P	Q	R	S	T	UV	W	Х	Y	Z
1 @timestamp		extension fi	le_info.SHA3-512	file_info.file_n	arfile_info.file_pati	file_info.file_type	file_info.	file_info.relative_path	has_expi	rissuer.common_name	issuer.co	u issuer.er	n issuer.lo	ic issuer.o	g issuer.o	rgnot_after	not_before	private_k	private_ks	public_ke public_	ke scan_id	self_signe	erial_nurs	ignature sul
2 2023-08-0972	0:00:24.391157	44	70eaaceb49ec755ecfi	0 ztecert.cer	/sample_C4.zip/e	UPEN_CERTIFICATE	/sample_	(eUSB/DR3/PkiRoot/vendor	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null	null	null	203612012151452	202112012151452	null	FALSE	2,048	6 63cd036c-	FALSE	2.33E+23 s	ha256WR 741
3 2023-08-0972	0:00:24.391157	44	70eaaceb49ec755ecfi	0 ztecert.cer	/sample_C4.zip/e	UPEN_CERTIFICATE	/sample_	(eUSB/DR3/1/swm/PkiRoot,	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null	null	null	203612012151452	202112012151452	null	FALSE	2,048	6 63cd036c-	FALSE	2.33E+23 s	ha256WR 741
4 2023-08-0912	0:00:24.391157	44	70eaaceb49ec755ecfi	0 ztecert.cer	/sample_C4.zip/e	UPEM_CERTIFICATE	/sample_	eUSB/DR3/1/bsa/PkiRoot/v	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null	null	null	203612012151452	202112012151452	null	FALSE	2,048	6 63cd036c-	FALSE	2.33E+23 s	ha256Wi 741
5																								
6																								
$\langle \rangle$	c4_certificat	es +																		_		_		

Figure 122: C4 Certificates Report (Jarvis)

		τ.	D E	F	G	H I		κ	1 M	N	0	Q	5	U W	AA	AB	AC .	ΔD.	4
1 affected_versit	ons certain	compone	CVR.095.V CVR.0955.	V CVN. EVSI	LV EVR. CVSS.V O	NR.CV55.V 298.CV55.V	CVV.CVES	v eve.cvss.y30.vecti cv	0.0155.V (Y0.0155.V	CVP.CVSS	v two.cvss.v31.vector	cve.name	ove.mid_info.published ove.mit	Linfo.upda cve.problem_types	file_list	fixed_in	product	product	vreasoning
2 [7.0.0, 7.881]	TRUE	libcurl	10 critical	TRUE	AV:N/ACI	8.8 high	TRUE	CV55:3.0/AV:N/A	8.8 high	FALSE	CV55:3.1/AV:N/ACI/PR:N/U:R/5:U/C:H/I:H/A:H	CVE-2023-27533	3/30/2023	4/21/2023 CWE-76	/sample_C4.zp/eUSB/DR3/luben/init_c.tar/938c858Fa405c	> 7.881	curl	7.66.0	Matched on pro-
1 [7.27.0, 7.78.0]	TRUE	libcuri	2.6 low	FALSE	AV:N/ACI	5.3 medium	TRUE	CV55:3.0/AV:N/A	5.3 medium	FALSE	CV55:3.1/AV:N/AC:H/PR:N/ULR/SU/C:H/EN/A/N	CVE-2021-22923	8/5/2021	1/5/2023 CWE-522	/sample_C4.zip/eUS8/DR3/luban/init_c.tar/938c958fa405c	>= 7.78.0	auri .	7.05.0	Matched on pro-
4 <7.85.0	TRUE	libcurt	2.6 low	TRUE	AV:N/AC:I	3.7 low	TRUE	CVSS:3.0/AV:N/A	3.7 low	FALSE	CV55:3.1/AV:N/AC:H/PR:N/UEN/S:U/C:N/I:N/ACL	CVE-2022-35252	9/23/2022	3/1/2023	/sample_C4.zip/eUSB/DR3/luban/init_c.tar/938c958fa405c	= 7.85.0	curl	7.66.0	Matched on pro-
5 <8.1.0	TRUE	libcurl	5.4 medium	TRUE	AV:N/AC:I	5.9 medium	TRUE	CV55:3.0/AV:N/A	5.9 medium	FALSE	CV55:3.1/AV:N/ACH/PR:N/UEN/S:U/C:N/EN/A:H	CVE-2023-28320	5/26/2023	6/9/2023 CWE-362, CWE-400	/sample_C4.zip/eUSB/DR3/luban/init_c.tar/938c958fa405c	=8.1.0	curt	7.66.0	Matched on pro-
6 <3.1.0	TRUE	libcurt	2.6 low	TRUE	AV:N/ACI	3.7 low	TRUE	CV55:3.0/AV:N/A	3.7 low	FALSE	CV55:3.1/AV:N/ACH/PR:N/UEN/S:U/CL/EN/A:N	CVE-2023-28322	5/26/2023	6/16/2023	/sample_C4.zip/eUSB/DR3/luban/init_c.tar/938c958fa405c	>= 8.1.0	curt	7.66.0	Matched on pro-
7 [1.18.0, 1.33.1]	TRUE	busybox	6.5 medium	FALSE	AV:N/AC:I	7.2 high	TRUE	CV55:3.0/AV:N/A	7.2 high	FALSE	CV55:3.1/AV:N/ACL/PR:H/UEN/S.U/CH/UH/A:H	CVE-2021-42379	11/15/2021	4/25/2023 CWE-416	/sample_C4.zip/eUSB/DR3/lubar/init_c.tar/9df239d952c8c	>1.33.1	busybox	1.31.1	Matched on pro-
	of curs												1.40				-	_	

## Figure 123: C4 CVEs (Jarvis)

@timesta domain	file info.MD5 file info	SHA-1 file info.5file info.5file info.5					fo.ffile info.ffile info.ffile info.ffile info.ffile info						string	
2023-08-01 lists.sourceforee.net		fc66F147c a850e9e6c4466574a55e64d194	TRUE	,mo			E D RegularFil 2023-08-07 /sample (usr/share, 63cd036c	0	33.261	40,791	0	translation-team-eo	translation-team-eoi0lists.sou	ceforze.ne
2023-08-0 gmail.com		b92f6ad4 04a51042: 68838d59: a6237bb7!	FALSE	mo			E D RegularFil 2023-08-07 /sample i usr/share/locale/zi			17,194	0	wantinghard	wantinghard@gmail.com	
2023-08-0' googlegroups.com		b92f6ad4 04a51042: 68838d59; a6237bb7!		mo			E D RegularFil 2023-08-07 /sample i usr/share, 63cd036c		33.261	17.194	0	(18n-zh	118n-zh@googlegroups.com	
2023-08-0rgmail.com		195024a2 51a49fae2 1ed3858ev d62683f2f					E D RegularFil 2023-08-07 /sample tusr/share/locale/ni		33.261	17,756	0	peterhamming	peterhamming@gmail.com	
2023-08-0: vrijschrift.org		1f6024a2 51a49fae2 1ed3858ev d62683f2f					E DRegularFil 2023-08-07 /sample (usr/share/locale/n		33.261	17,756	0	vertaling	vertaling@vrijschrift.org	
2023-08-0 vnijschrift.org		19024a2 51a49fae2 led 1858e d62683f2f	TRUE	.mo			E D RegularFil 2023-08-07 /sample_tusr/share, 63cd036c		13,261	17,756	0	vertaling	vertaling@vrijschrift.org	
2023-06-07.d07.ru		db466ad 4d356c3ex1e6719465 19c6d9dd					E D RegularFil 2023-08-07 /sample / usr/share, 63cd036c			24,561	0	enu	gnu@d07.ru	
2023-08-0*gmail.com		1914e881 7fx90defa 06aeede4 4e70dc244					E D RegularFil 2023-08-07 /sample 1 usr/share/locale/tr		33,261	14.020	0	ozgursarier1011601115	ozgursarier1011601115@gmail.	00.00
2023-08-0: gmail.com		73e460b6632c73529126cee3950c970e2fb					E DRegularFil 2023-08-07 /sample_fusi/filine/locale/gl		33.261	17.653	0	leandro.regueiro	leandro.regueiro@gmail.com	
2023-08-0 amail.com		73e460b6632c73529126cee39f0c970e2fb					E DRegularFil 2023-08-07 /sample_tusr/share, 63cd036c		33,261	17.653	~	leandro.regueiro	leandro.regueiro@gmail.com	
2023-08-0 trasno.net		73e460b6632c73529126cee39:0c970e2fb		.00			E D Regularfil 2023-08-0: /sample_tusr/share, 63cd036c		33,261	17,653	0	proxecto	proxecto@trasno.net	
2023-08-0: gmail.com		ba4eea8:2b6d789brbdcf711d2677660fdf					E D RegularFil 2023-08-07 /sample_fusr/share_63cd036c E D RegularFil 2023-08-07 /sample_fusr/share_63cd036c		33,261	19,535	0	rffontenelle	rffontenelle@gmail.com	
2023-08-0*gmail.com		12fe4846 300cfcde0 365ef2684 o4b27227e	FALSE	.mo			E D RegularFil 2023-08-07 /sample_tusr/share/locale/e		33,261	19,555		abelnicolas1976	abelnicolas1976@gmail.com	
		szne4846 soucricised secenze84 o46272274 32fe4846 soucricised secenze84 o46272274	TRUE	.mo					33,261	19,231	0	abelnicolas1976		
2023-08-0'gmail.com							E_D RegularFil 2023-08-07 /sample_Lusr/share, 63cd036c				0		abelnicolas1976@gmail.com	
2023-08-01 linux.hr		04308146: da8730183.52718afa5 caf5e0fde		,mo			E_D RegularFil 2023-08-07 /sample_i usr/share, 63cd036c		33,261	18,615		lokalizacija	lokalizacija@linux.hr	
2023-08-01 sudio.ws		5907b1d #887b476 5d90c1538 be214f46f	TRUE				_TEI RegularFil 2023-08-0: /sample_tusr/share, 63cd036c		33,261	4,499	0	sudo	sudo@sudo.ws	
2023-08-01 mehmetkececi.com		1d7f9a04 23f66d01Ecba9c71697b43177cc		,mo			E_D RegularFil 2023-08-07/sample_i usr/share, 63cd036c		33,261	18,557	0	mkececi	mkececi@mehmetkececi.com	
2023-08-01 lists.sourceforge.net		7b6b0832010595d2xdee0ec78x3f4e717ae		.mo			E_D RegularFil 2023-08-07 / sample_i usr/share, 63cd036c		33,261	19,870	0	translation-team-fi	translation-team-fi@lists.sour	etorge_net
2023-OB-0: huftis.org		593c32c0 7453b7b6ib7b5166d b7473169k	TRUE	.mo			E_D RegularFil 2023-08-0: /sample_i usr/share, 63cd036c		33,261	3,058	0	karl	karl@huftis.org	
2023-08-0: lister.ping.uio.no		593c32c0 7453b7b6ib7b5166d b7473169k		.00.			E_D RegularFil 2023-08-07 /sample_t usr/share/locale/n		33,261	3,058	0	i18n-nn	i18n-nn@lister.ping.uio.no	
2023-08-0t us.oracle.com		2e35470:d2761426:7b189b35:0e8822cb7					_TE: RegularFil 2023-08-0: /sample_t usr/share, 63cd036c		33,261 1		0	bjjackso	bjjackso@us.oracle.com	
2023-08-0 cdu.elektra.ru	c5d6a7a8a0f3bc5588fa7bff64i3343ba9	2e35470xd2761426;7b185b35;0e8822cb7	FALSE				_TEI RegularFil 2023-08-0/ /sample_i usr/share/doc/sudi		33,261 1	,416,627	0	ppz	ppz@cdu.elektra.ru	
2023-08-0t openbsd.org		2e35470:d2761426:7b189b35:0e8822cb7					TEI RegularFil 2023-08-07 /sample_1 usr/share, 63cd036c		33,261 1		0	espie	espie@openbsd.org	
2023-08-0:tsd.edu	c5d6a7a8a0f3bc5588fa7bff64i3343ba9	2e35470:d2761426:7b189b35:0e8822cb;	TRUE		ChargeLo, UTF-8 Univ	/sample_CUTF_8	TEI RegularFil 2023-08-0: /sample_tusr/share, 63cd036c	- 0	33,261 1	,416,627	0	drno	dmo@tsd.edu	
2023-08-01 cs. colorado.edu	c5d6a7a8a0f3bc5588fa7bff64;3343ba9	2e35470: d276142657b189b35: 0e8822cb1	FALSE		ChangeLo, UTF-8 Univ	/sample_tUTF_8	TE: RegularFil 2023-08-07 /sample_tusr/share/doc/sude	0	33,261 1	416,627	0	sudo-bugs	sudo-bugs@cs.colorado.edu	
2023-08-0 dl5000.bc.edu	c5d6a7a8a0f3bc5588fa7bff64i3343ba9	2e35470:d2761426;7b189b35;0e8822cb;	TRUE		ChangeLo, UTF-8 Unit	/sample_CUTF_8	TE: RegularFil 2023-08-0/ /sample_i usr/share, 63cd036c	- 0	33,261 1	416,627	0	John_Rouillard	John_Rouillard@dl5000.bc.edu	
2023-08-0:cs.umb.edu	c5d6a7a8a0f3bc5588fa7bff64i3343ba9	2e35470: d2761426: 7b189b35: 0e8822cb7	FALSE		ChangeLo, UTF-8 Unit	/sample_CUTF_8	TE: RegularFil 2023-08-0: /sample_iusr/share/doc/sudi	0	33,261 1	416,627	0	rouili	rouil(@cs.umb.edu	
2023-08-0t lists.sourceforge.net	cc325ae613d695b8ccc9bfa89c 63031bf6	3cfd5b6a 4e1d1cc7315b351c5c3e041d76i	TRUE	.mo	sudpers.rr GNU mess	/sample (LOCALF	E D RegularFil 2023-08-0/ /sample tusr/share, 63cd036c	- 0	33,261	6,445	0	translation-team-eu	translation-team-eu@lists.sou	ceforge.ne
2023-08-0 openbsd.org	c5d5a7a8a0f3bc5588fa7bff64i3343ba9	2e35470:d2761426;7b189b35:0e8822cb7	FALSE		ChangeLo UTF-8 Unix	/sample (UTF 8	TE: RegularFil 2023-08-07 /sample Tusr/share/doc/sudi	0	33,261 1	416,627	0	djm	djm@openbsd.org	
2023-08-0 gistnet.com	c5d6a7a8a0f3bc5588fa7bff64i3343ba9	2e35470: d2761426; 7b189b35; 0e8822cb;	FALSE		ChangeLo UTF-S Unic	/sample (UTF 8	TEI RegularFil 2023-08-07 /sample 1usr/share/doc/sudi	0	33,261 1	416.627	0	mike	mikes@gistnet.com	
2023-08-0: cs.few.eur.nl	c5d6a7a8a0f3bc5588fa7bff64c3343ba9l	2e35470xd2761426;7b189b35.0e8822db;	FALSE		ChangeLo UTF-8 Unit	/sample (UTF 8	TEI RegularFil 2023-08-07 /sample tusr/share/doc/sudi	0	33.261 1	416.627	0	pk	ok@cs.few.eur.nl	
2023-08-0t reppep.com	c5d6#7#8#0f3bc5588f#7bff64/3343ba9	2e35470: d2761426" 7b189b35: 0e8822cb;	TRUE		ChangeLo UTF-8 Unit	/sample suTF 8	TEI RegularFil 2023-08-07 /sample Tusr/share, 63cd036c	- 0	33,261 1	416.627	0	pepper	pepper@reppep.com	
2023-08-07 linnaean.org	r5d6a7a8a0f3hr5588fa7hff64;3343ha9	2e35470xd276142657b189b35.0e8822cb;	FALSE				TE: RegularFil 2023-08-0: /sample (usr/share/doc/sudi		33.261 1	416 627	0	hag	hag@linnaean.org	
2023-08-07 headgear.org	c5cHa7a8a0f3bc5538fa7bff64,3343ba9	2e35470cd276142617b189b35.0e8822cb1	FALSE				TEI RegularFil 2023-08-07 /sample 1 usr/share/doc/sudi		33.261 1	416.677	0	doyce	cloyce@headgear.org	
2023-08-01cs.dal.ca		2e15470:d2761426"7b189b35"0e8822cb;					TEI RegularFil 2023-08-07 /sample i usr/share/doc/sudi		33.261 1		0	aaron	aaron@cs.dal.ca	
2023-08-0 email.com		2+15470xd2761426"7b189b15:0+8822cb7	FALSE				TE: RegularFil 2023-08-07 /sample_tusr/share/doc/sudi		13,261 1		0	beuillory	bguillory@email.com	
2023-08-0 email.com		2e35470:d2761426;7b189b35;0e8822cb;	TRUE				TE: RegularFil 2023-08-07 /sample (usr/share, 63cd036c		33,261 1		0	bguillory	bguillory@email.com	
2023-08-0 rte.com.cn		0732bb724ff611fd 8ac8933df 1719a335E		.000041b1	GZIP DECIELF 64-bit		RegularFil 2023-08-07 /sample (GZIP DEO 63cd036c		33,188 =		0	Open.Source	Open.Source@zte.com.cn	
2023-06-0 vper.kernel.org		0f732bb724ff611fd 8ac8933df 1719a335E	TRUE	.000041b1	GZIP DECIELF 64-bit		RegularFil 2023-08-07 /sample + G2IP DEO 63cd036c		33.188 #			linux-kernel	linus-kernel@vzer.kernel.orz	
2023-08-0 vger kernel.org		0f732bb224ff611fd_8ac8933df 1719a335E		.000041b1	GZIP DECIELF 64-bit		RegularFil 2023-08-0: /sample_1621P_DE0 63cd036c		33,188 #		0	linux-scpi	linux-acpi@vger.kernel.org	
2023-08-0 vger.kemel.org		0732bb234ff611fd Bac8933df 1719a335e		.000041b1	GZIP DECIELF 64-bit		RegularFil 2023-08-07 /sample 1621P DECOMPRESS		13,160 #		0	linux-scsi	linux-scsi@vger.kemel.org	
2023-08-0 alpha franken de		0732bb224ff611fd:8ac8933df1715a335E		.00004151					33,188 #		0			
					GZIP_DEC/ELF 64-bit		RegularFil 2023-08-07 / sample_i G2IP_DECOMPRESS				0	tsbogend	tsbogend@alpha.franken.de	
2023-06-0/vger.kernel.org		0f732bb224ff611fd.8ac8933df1719a3358		.000041b1	GZIP_DECIELF 64-bit		RegularFil 2023-08-0: /sample_IG2IP_DECOMPRESS		33,188 #		0	linux-usb	linux-usb@vger.kernel.org	
2023-08-0:vger.kernel.org		0f732bb224ff611fd18ac8933df1719a3358			GZIP_DECIELF 64-bit		RegularFil 2023-08-07 /sample_1G2IP_DEO 63cd036c		33,188 #			linux-usb	linux-usb@vger.kernel.org	
2023-08-01 redhat.com		0F732bb224ff611fd Bac8933df 1719a3358	FALSE	.000041b1	GZIP_DECIELF 64-bit		RegularFil 2023-08-07 /sample_I GZIP_DECOMPRESS			*****	0	dm-devel	dm-devel@redhat.com	
2023-08-01gzip.org		5b568efc1f17c9b9c ead0d0d5 ba7d4d1e					5E_F RegularFil 2023-08-07 /sample_i usr/share, 63cd036c		33,261	9,899	0	foup	jloup@gzip.org	
2023-08-0: alumni.caltech.edu		5b968efc1f17c9b9cead0d0d5ba7d4d1e					SE_FRegularFil 2023-08-07/sample_iusr/share/doc/sudi		33,261	9,899	0	madler	madler@alumni.caltech.edu	
2023-08-0: dansk-gruppen.dk		cf6e3fb0.cc97acc52i3b980f41b05bebaf9k	FALSE	,mó			E_D RegularFil 2023-08-0: /sample_i usr/share/locale/di		33,261	18,049	0	dansk	dansk@dansk-gruppen.dk	
2023-08-0: courtesan.com		da69863 aab8d4a4i db33c2eei 126318d68	TRUE		HISTORY ASCII text		RegularFil 2023-08-07 /sample_t usr/share, 63cd036c		33,261	2,928	0	Todd.Miller	Todd.Miller@courtesan.com	
2023-08-01 Mv.Fk		fbc58efa: f6d89089755b30b4ct 619bcf914		.589			OW RegularFil 2023-05-1: /sample_ieUSB/DR3/BIN/cpu			SUSSIAN .	1,000	KR	KR@Mv.Fk	
2023-08-0: W.To		fbc58efa. f6d89089755b30b4ct 619bcf914					OW RegularFil 2023-05-1: /sample_reUSB/DR3/BIN/opu				1,000	n	n@W.To	
2023-08-0: gmail.com		d13a002238e6dc80Caf665b1ch5e084dc16	TRUE	.mo			E_D RegularFil 2023-08-0: /sample_i usr/share, 63cd036c	- 0	33,261	21,485	0	vnwildman	vnwildman@gmail.com	
2023-08-0 lists.sourceforee.net	651099a55f2d789b835d1c736:75309b0		FAISE				E D.RegularFil 2023-08-0t /sample +usr/share/locale/pl	/ 0	33.261	19.369	0	translation-team-ol	translation-team-pl@lists.sour	

## Figure 124: C4 email addresses (Jarvis)

A	B	C	D	E	F	1.1	K	L	М	Ν	0	P	Q
@timestamp	cracked_pw	file_info.SHA3-512	file_info.file_name	file_info.file_path	file_info.	f file_info.tgid	homedir	password	realname	scan_id	shell	uid	username
2023-08-09T20:00:25.951303		95c9f43debf825516dcac0747fb868e	shadow	/sample_C4.zip/eUSB/DR4/ramdisk.bin/FILE/etc/shadow	ASCII	2023-08-0	0/	\$5\$SSkzbWaJ\$07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXIMeL016	Linux Administrator	63cd036c	:-/bin/sh		0 zte
2023-08-09T20:00:25.951303		95c9f43debf825516dcac0747fb868e	shadow	/sample_C4.zip/eUSB/DR5/ramdisk.bin/FILE/etc/shadow	ASCII	2023-08-0	0/	\$5\$uFWcf7Dq\$isiMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	Linux Administrator	63cd036c	:-/bin/sh		0 admin
2023-08-09T20:00:25.951303		95c9f43debf825516dcac0747fb868e	shadow	/sample_C4.zip/eUSB/DR4/ramdisk.bin/FILE/etc/shadow	ASCI	2023-08-0	0/	\$5\$uFWcf7Dq\$isiMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	Linux Administrator	63cd036c	:-/bin/sh		0 admin
2023-08-09T20:00:26.208018	NO PASSWORD	5c575a810e1c548e392b4740cdc9a7	bitmaps.o	/sample_C4.zip/eUSB/DR5/ramdisk.bin/FILE/lib/libext2fs.a/bitmaps.o	OBJECT_F	2023-08-0	0 /raat		Linux User,	63cd036c	:-/bin/sh		0 root
2023-08-09T20:00:26.208018	NO PASSWORD	5c575a810e1c548e392b4740cdc9a7	bitmaps.o	/sample_C4.zip/eUSB/DR4/ramdisk.bin/FILE/lib/libext2fs.a/bitmaps.o	OBJECT_F	2023-08-0	0 /root		Linux User,	63cd(36c	:-/bin/sh		0 root
2023-08-09T20:00:25.951303		95c9f43debf825516dcac0747fb868e	shadow	/sample_C4.zip/eUSB/DR5/ramdisk.bin/FILE/etc/shadow	ASCII	2023-08-0	0/	\$5\$\$\$kzbWaJ\$07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXIMeL016	Linux Administrator	63cd(036c	:- /bin/sh		0 zte
2023-08-09T20:00:25.951303		95c9f43debf825516dcac0747fb868e	shadow	/sample_C4.zip/eUSB/DR5/ramdisk.bin/FILE/etc/shadow	ASCII	2023-08-0	1 /var/emp	el la	Linux User,	63cd((36c	-/usr/sbin/nologin	1,00	11 sshd
2023-08-09T20:00:25.951308		95c9f43debf825516dcac0747fb868e	shadow	/sample_C4.zip/eUSB/DR4/ramdisk.bin/FILE/etc/shadow	ASCIL	2023-08-0	1 /var/emp	1	Linux User,	63cd036c	-/usr/sbin/nologin	1,00	11 sshd

## Figure 125: C4 Password File Analysis (Jarvis)

@timesta file info.MD5					HL.	N 10	8.	80			-17	80 8	NL PL	88	50
	file_info.5HA-1_file_info.5file_info.5file_info.5file_info	o.ffile_info.file_path	file_info.gfile_info.	.mod_timestampfile_	info.stat.gid file	info.stat.u fragment	netioc	path	string						
2023-08-0 796164133977c5aacb483af	e12621a0x2f11c3 01e3f9477 befbf90b89d9e2e36 dv-lte.j	soi/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:27:23	1,000	1,000	www.amazon.on		www.amazo	n.on					
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000	git.k8s.io	/community/contributors/devel/api-conventions.mdMessage	https://git.k	Bs.io/comm	unity/cor	tributors/dev	rel/api-com	entions.md	Message
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 spec-and-statusLocalObjectRefe	rgit.k8s.io	/community/contributors/devel/api-conventions.md	https://git.k	ls.ia/comm	unity/cor	tributors/dev	rel/api-com	entions.md	#spec-and-sta
2023-06-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcdbe20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 spec-and-statuspublicsuffix.org	sgit.k8s.io	/community/contributors/devel/api-conventions.md	https://git.k	Bs.io/comm	unity/cor	tributors/dev	rel/api-com	entions.md	Rspec-and-sta
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 nfsverbs	kubernetes.io	/docs/concepts/storage/volumes	https://kube	rnetes.io/a	iocs/cono	epts/storage/	volumes#nf	werbs	
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000	kubernetes.io	/docs/concepts/overview/working-with-objects/namespaces/#	le https://kubi	rnetes.io/u	iocs/cono	epts/overviev	v/working-w	ith-objects	/namespaces
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 emptydirOptional	kubernetes.io	/docs/concepts/storage/volumes	https://kube	rnetes.io/o	locs/cono	pts/storage/	volumester	nptydir0ptic	onal
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000 pod-conditionsA	kubernetes.io	/docs/concepts/workloads/pods/pod-lifecycle	https://kube	rnetes.io/u	locs/cono	epts/workloa	ds/pods/poi	Hifecycle#p	pod-condition
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 capacity/tems	kubernetes.io	/docs/concepts/storage/persistent-volumes	https://kubi	rnetes.io/c	locs/cono	pts/storage/	persistent-v	olumestkap	pacityItems
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000 spec-and-statusNodeResources	git.k8s.lo	/community/contributors/devel/api-conventions.md	https://git.k	Bs.io/comm	unity/cor	tributors/dev	rel/api-com	entions.md	Rspec-and-sta
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000	releases.k8s.io	/HEAD/docs/design/resources.md	http://relea	ies.k8s.io/H	EAD/doc	/design/reso	urces.md		
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca3 3d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000 gcepersistentdiskiP	kubernetes.ia	/docs/concepts/storage/volumes	https://kube	rnetes.io/u	iocs/cono	epts/storage/	volumes#gc	epersistenti	diskIP
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 pod-conditionsAccessModes	kubernetes.io	/docs/concepts/workloads/pods/pod-lifecycle	https://kube	rnetes.io/i	locs/cono	epts/workloa	ds/pods/por	Hifecycle#p	pod-condition
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca3 3d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000	kubernetes.ia	/docs/concepts/configuration/secretHost	https://kube	rnetes.io/i	iocs/cono	epts/configur	ation/secret	Host	
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000	kubernetes.io	/docs/concepts/configuration/manage-compute-resources-con	ta https://kube	rnetes.io/i	locs/cono	epts/configur	ation/manaj	etuqmoo-ei	-resources-co
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca3 3d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000	kubernetes.ia	/docs/tasks/configure-pod-container/configure-service-account	t/ https://kube	rnetes.io/i	iocs/tasks	(configure-pr	od-containe	/configure-	service-accou
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 restart-policyConfigMapEruSour	kubernetes.ia	/docs/concepts/workloads/pods/pod-lifecycle/	https://kube	rnetes.io/i	locs/cono	epts/workloa	ds/pods/por	Hifecycle/#	Restart-policy
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca3 3d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000	man7.org	/linux/man-pages/man5/machine-id.5.htmlFinalizers	http://man7	.org/linux/	nan-page	;/man5/mach	ine-id.5.htr	iFinalizers	
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 create-a-podPeriodic	releases.k8s.io	/HEAD/examples/volumes/glusterfs/README.md	https://relea	ises.k8s.io/	HEAD/ena	mples/volum	ies/glusterf:	(READNE.m	ndAcreate-a-p
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000 persistent-volumesRequired	kubernetes.io	/docs/concepts/storage/persistent-volumes	https://kube	rnetes.io/a	iocs/cono	pts/storage/	persistent-v	olumes#per	rsistent-valur
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 gcepersistentdiskA	kubernetes.ia	/docs/concepts/storage/volumes	https://kube	rnetes.io/u	iocs/cono	epts/storage/	volumesAgo	epersistento	diskA
2023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000 persistent-volumesTTY	kubernetes.io	/docs/concepts/storage/persistent-volumes	https://kube	rnetes.io/k	iocs/cono	pts/storage/	persistent-v	olumes#per	rsistent-valur
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efElpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12T14:28:47	1,000	1,000 updating-imagesThe	kubernetes.ia	/docs/concepts/containers/images	https://kube	rnetes.io/o	iocs/cono	epts/containe	rs/images#i	pdating-im	agesThe
023-08-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182efEipm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000 emptydirAdapts	kubernetes.io	/docs/concepts/storage/volumes	https://kubi	rnetes.io/s	locs/cono	pts/storage/	volumester	ıptydir Adap	ats
2023-08-0: fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182ef8lpm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000	kubernetes.io	/docs/concepts/configuration/assign-pod-node/MaxLimitRequ	es https://kube	rnetes.io/o	locs/cono	epts/configur	ation/assign	-pod-node/	MaxLimitRep
2023-06-0 fadd85ced90d229e9f44a2	d6a39c5c494fbcd be20d3b3 e04796ca33d9182ef8 [pm	/sample_C4.zip/eUS8/DR3/	RegularFil 2023-05-1	12714:28:47	1,000	1,000	kubernetes.io	/docs/concepts/overview/working-with-objects/labels/Filesyst							
c) c4 url-strings	in sourcessily of conducts contract states and the	lange of a large best	number i nen er e		1.000	a sea and a state to sea altern	historica da casa da c	false former and an end for extra the set of the set	Sec. 18. 4.						

Figure 126: C4 Infoleak URL Report (Jarvis)

4 → TEST ∽					Dov	wnload ~
verview Bill of Materials Findings Scans	Files					
Risk		Details				
<b>98</b> / 100 0 10 35 65	100	Operating Systems 👌 Linux Kernel 4.19.31 an	id Linux	Kernel	4.19.82	
	•	VxWorks Unknown				
Findings Detected 3,553		Architectures -				
		Products Depending On Th	nis Artif	act		
Software Components		August 2023				100
845		Created charles.begian@ngc.	com			
		August 30, 2023				
Finding Exploit Intelligence		Remediation Guidance	0			
Category	l₹ Count	Guidance	17	Assoc	ciated Fi	indings
✓ No Known Exploits	2,455 findings			-	-	_
Proof of Concept Exploit	01,058 findings	Address high risk component Linux Kernel 4.19.31	1	15	64	694
4 Weaponized	③ 40 findings	Address high risk component Linux Kernel	0	6	53	683
Reported in the Wild	③ 14 findings	4.19.82				
Exploited By Threat Actors	③ 8 findings	Address high risk component glibc-devel 2.17	2	18	80	48
		Address high risk component python27- python-test 2.7.13	0	8	34	28

# Sample C4 Finite State Platform Scan Report Excerpts

Figure 127: C4 Scan Overview (Finite State Platform)

C4 > TEST ~ Overview Bill of Materials Findings Scans	s File	es			Dov	vnload \vee 🛛 Upload
Findings by Severity 3,553 findings • Low (2531) • Medium (825) • High (181) • Critical (1			Category No Kno Proof of Weaport	ploit Intelligence own Exploits of Concept Exploit nized ed in the Wild ed By Threat Actors		IF Count 2,455 findings ⊙ 1,058 findings ⊙ 40 findings ⊙ 14 findings ⊙ 8 findings
<b># Filter</b> Q Search findings						:
Title		Severity	≕ Risk Status	CVE	CWE	Found By
CVE-2015-0235 - glibc-devel:2.17	ଡ	Critical	<b>10</b> /10	CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2015-0235 - glibc-devel:2.17	ଡ	Critical	<b>10</b> /10	CVE-2015-0235	CWE-787	Finite State Monitoring
CVE-2019-3822 - cURL:7.55.1	ර	Critical	9.5/10	CVE-2019-3822	CWE-787	Finite State Monitoring
CVE-2022-1292 - OpenSSL:1.1.1d	ර	Critical	<b>9.5</b> /10	CVE-2022-1292	CWE-78	Finite State Monitoring
CVE-2022-1292 - openssl-libs:1.1.1c	ଡ	Critical	9.5/10	CVE-2022-1292	CWE-78	Finite State Monitoring
CVE-2022-1292 - OpenSSL:1.0.2n	ර	Critical	9.5/10	CVE-2022-1292	CWE-78	Finite State Monitoring
CVE-2019-10125 - Linux Kernel:4.19.31	Ø	Critical	<b>9.4</b> /10	CVE-2019-10125	CWE-416	Finite State Monitoring

Figure 128: C4 Findings (Finite State Platform)

D	E
category	subcategory
CREDENTIALS	PASSWD_USER_ACCOUNTS
CRYPTO_MATERIAL	PEM_CERTIFICATE_KEY
SAST_ANALYSIS	HEAP_BUFFER_OVERFLOW
SAST_ANALYSIS	DOUBLE_FREE
CONFIG_ISSUES	SSH_PERMIT_ROOT
SAST_ANALYSIS	UNCHECKED_RETURN_VALUE
CONFIG_ISSUES	SSH_MAX_RETRIES
SAST_ANALYSIS	EXPRESSION_ALWAYS_TRUE
SAST_ANALYSIS	INHERENTLY_DANGEROUS_FUNCTION
SAST_ANALYSIS	IMPROPER_LENGTH_HANDLING
SAST_ANALYSIS	INCORRECT_BEHAVIOR_ORDER
SAST_ANALYSIS	VERY_HIGH_CODE_COMPLEXITY
SAST_ANALYSIS	HIGH_CODE_COMPLEXITY
CREDENTIALS	SHADOW_HARD_CODED_PASSWORDS
CREDENTIALS	PASSWD_HARD_CODED_PASSWORDS
CONFIG_ISSUES	SELINUX_DISABLED
CRYPTO_MATERIAL	PKCS8_PRIVATE_KEY
SAST_ANALYSIS	VXWORKS_EXE_NO_PASSWORD
SAST_ANALYSIS	STACK_BUFFER_OVERFLOW
CVE	KNOWN_VULNERABILITIES
C4_TEST	findings +

Figure 129: C4 Findings Categories (Finite State Platform)

А	В	С	D	G	Н	1
/ulnIdFromTool	riskScore cv	ssV3Score	cvssVectorString	affectedComponents	exploitCount	maxExploitMaturit
CVE-2022-0435	7.2	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:4.19.82	2	рос
CVE-2019-11479	7.5	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.19.31	1	рос
CVE-2019-10125	9.4	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:4.19.31	1	рос
CVE-2019-11478	7.5	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.19.31	1	poc
CVE-2019-11477	7.5	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Linux Kernel:4.19.31	1	рос
CVE-2022-0435	7.2		CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	Linux Kernel:4.19.31		poc
CVE-2017-3730	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		рос
CVE-2016-7054	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		рос
CVE-2016-6304	7.2		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		рос
CVE-2016-6305	7.2		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		poc
CVE-2016-8610	7.3		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		рос
CVE-2017-3730	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		poc
CVE-2016-8610	7.3		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		poc
CVE-2016-6305	7.2		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		poc
CVE-2016-7054	7.4		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		poc
CVE-2016-6304	7.2		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.0		poc
CVE-2020-1967	7.2		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	OpenSSL:1.1.1d		poc
CVE-2022-1292	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.1.1d		рос
CVE-2022-1232 CVE-2018-20843	7.4		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	libexpat1-dev:2.2.0-2+deb9u3		poc
CVE-2018-20845	7.4		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	libexpat1-dev:2.2.0-2+deb9u3		poc
CVE-2022-25315 CVE-2022-25236	8.7		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	libexpat1-dev:2.2.0-2+deb9u3		poc
CVE-2022-25236 CVE-2019-5436	7.3		CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.55.1		poc
CVE-2019-3430 CVE-2019-3822	9.5			cURL:7.55.1		
CVE-2019-3822 CVE-2018-0500	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	cURL:7.55.1		рос
			CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H			рос
CVE-2018-20843	7.4		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	expat:2.2.0		рос
CVE-2022-25315 CVE-2022-25236	7.3		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	expat:2.2.0		рос
	8.7		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	expat:2.2.0		рос
CVE-2021-43527	7.3		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	NSS:3.12.4		рос
CVE-2022-1292	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	OpenSSL:1.0.2n		poc
CVE-2023-38408	8.9		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	openssh-dbg:8.3_p1-r1		weaponized
CVE-2023-38408	8.9		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	openssh-dbg:8.3_p1-r1		weaponized
CVE-2018-15514	8.4		CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	docker-client:1.13.1		рос
CVE-2018-15514	8.4		CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	docker-client:1.13.1		рос
CVE-2021-3156	7.8		CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	sudo-devel:1.8.22		weaponized
CVE-2019-14287	7.7		CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	sudo-devel:1.8.22		weaponized
CVE-2018-1000802	7.8		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	python27-python:2.7.13		рос
CVE-2018-1000802	7.8		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	python27-python:2.7.13		рос
CVE-2022-1292	9.5		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	openssl-libs:1.1.1c		рос
CVE-2021-43527	7.3		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	nss-util:3.16.2.3		рос
CVE-2021-3156	7.8		CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	sudo:1.8.22		weaponized
CVE-2019-14287	7.7		CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	sudo:1.8.22		weaponized
CVE-2019-19844	9.3		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	django-tools:0.32.10	4	рос
CVE-2018-20843	7.4		CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	libexpat:2.2.0-1		рос
CVE-2022-25315	7.3	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	libexpat:2.2.0-1	1	рос
CVE-2022-25236	8.7	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	libexpat:2.2.0-1	1	рос
CVE-2015-8779	8.6	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc-devel:2.17	1	рос
CVE-2015-0235	10			glibc-devel:2.17	29	weaponized
CVE-2014-9402	7.4			glibc-devel:2.17	3	рос
CVE-2014-9984	8.5	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc-devel:2.17	2	рос
CVE-2014-9761	8.7	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc-devel:2.17	2	рос
CVE-2015-8778	8.4	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc-devel:2.17	1	рос
CVE-2015-7547	8.1	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc-devel:2.17	18	weaponized
CVE-2015-7547	8.1	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	glibc-devel:2.17	18	weaponized
< > C4	TEST.exploit-ir	atol	+			

Figure 130: C4 CVE Exploitability (Finite State Platform)

# **APPENDIX G: CST SCAN REPORT EXCERPTS FOR SAMPLE C5**

#### Black Duck Binary Analysis Search and jump to group. 🕹 Upload 🛛 🝷 은 charles.begian sample\_C5.zip Vulnerability analysis Information leakage Executable attributes Static code analysis Details Feed Analysis settings File content General Name sample\_C5.zip 🖉 Description No description given 🗹 Version No version given 🖉 2023-08-10 14:37 (4 days ago) by charles.begian Uploaded 2023-08-10 14:39 (4 days ago) Last scanned 20230608 BDBA engine version used for scanning BDBA frontend version used for calculation 20230615 LATEST Protect from data retention Notify on new vulnerabilities **File properties** File 👍 Replace File available No SHA1 b0802e82757a89a85cfabd50be88990374d21687 Size 66.5 MB (original) / 194.11 MB (scanned) Analysis © Remove Application type Virtual machine image Duration 2 minutes Throughput ③ 1.23 GB/s 2023-08-14T11:59:50 STALE BDSA database version ③ 2023-08-14T06:15:00 STALE NVD database version ③ 2023-08-14T04:04:31 Component database version ④ 2023-05-31T10:04:47 Native fingerprint version Low risk tolerance mode No 🛈 Include historical vulnerabilities Yes 🛈 CVSS v3 missing score fallback No 🛈

# Sample C5 Black Duck Scan Report Excerpts

Figure 131: C5 Scan Overview (Black Duck)

# sample\_C5.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY

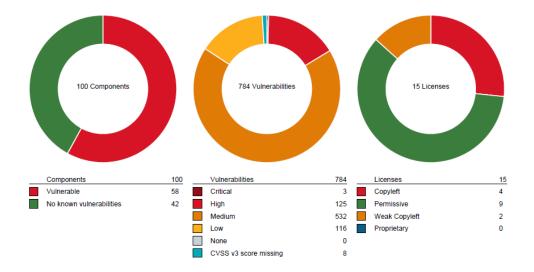


Figure 132: C5 Scan found 784 Vulnerabilities (Black Duck)

Details		
Original filename SHA1 checksum Original file size	b0802e82757a89a85cfabd50be88990374d21687 66.5 MB	
Infoleak		
Asymmetric keys:	21	
AWS keys:	0	
Custom pattern matches:	0	
Emails:	308	
HTTP authentication:	0	
Image metadata:	0	
IP addresses:	249	
JSON web tokens:	0	
MAC addresses:	2	
OAuth tokens:	0	
Passwords:	2	
Shell history:	0	
URLs:	728	
Twilio keys:	0	
Google cloud keys:	0	
This result is a product of an automatic	analysis and may contain errors or omissions.	Page 16/17

Report generated 2023-08-14T00:07:15Z https://protecode-sc.com/products/24699143

Facebook access tokens: 0

Figure 133: C5 Information leaks (Black Duck)

	А	В	С	D	E	F	G	н	1.1	J	K	L	M	N	0	P	Q	R
1	Algorithm	n Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File							
2	RSA	51	2 DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	_C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/bin/op	enssl']	
3	RSA	409	5 PEM	TRUE	FALSE	'BEGIN RSA PRIVATE KEY					['sample	_C5.zip',	'BB6648.img',	partition-	0/initrd',	'lib64/librh	ai_vc.so.0.	D.O']
4	ECDSA	25	5 PEM	TRUE	FALSE	'BEGIN EC PRIVATE KEY					['sample	_C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/lib64/l	ibgnutls.so	.30.22.0']
5	RSA	204	B DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/bin/op	enssl']	
6	RSA	307	2 DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	_C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/bin/op	enssl']	
7	DSA	51	2 PEM	TRUE	FALSE	'BEGIN DSA PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/lib64/l	ibgnutls.so	.30.22.0']
8	RSA	204	B PEM	TRUE	FALSE	BEGIN RSA PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/lib64/l	ibgnutls.so	.30.22.0']
9	RSA	1536	D DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/bin/op	enssl']	
10	RSA	409	5 DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/bin/op	enssl']	
11	RSA	768	DER	TRUE	FALSE	'BEGIN PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	, 'partition-	0/initrd',	'usr/bin/op	enssl']	
12	RSA	102	4 DER	TRUE	FALSE	BEGIN PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/bin/op	enssl']	
13	ECDSA	25	5 PEM	TRUE	FALSE	'BEGIN EC PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	partition-	0/initrd',	'usr/lib64/l	ibgnutls.so	.30.22.0']
14	DSA	204	B PEM	TRUE	FALSE	BEGIN DSA PRIVATE KEY					['sample	C5.zip',	'BB6648.img',	, 'partition-	0/initrd',	'usr/lib64/l	ibgnutls.so	.30.22.0']
15																		
	< >	C5	infoleak-a	symmetric	-private	+												

## Figure 134: C5 Asymmetric keys (Black Duck)

A	8 C	D	E	F	G	н	1.1	L	
Algorithm	Bits Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	file
RSA	2048 PGP key	FALSE	FALSE	BEGIN PGP PUBLIC KEY BLOCK		2020-10-30T08:14:17			['sample_C5.zip', '886648.img'
RSA	4096 PEM	FALSE	FALSE	'BEGIN PUBLIC KEY		2041-04-16712:13:45	TRUE	["countryName": "SE", "stateOrProvinceName": "Stockholm", "organizationName": "Ericsson", "organizationalUnitName": "RCS", "commonName": "DUMMT1234.ericsson.com"}	['sample_C5.zip', '886648.img'
RSA	2048 PGP key	FALSE	FALSE	'BEGIN PGP PUBLIC KEY BLOCK		2019-12-31T11:01:23			['sample_C5.zip', '886648.img'
RSA	2048 PEM	FALSE	FALSE	'BEGIN PUBLIC KEY		2036-01-22T09:55:15	TRUE	["countryName": "SE", "stateOrProvinceName": "Stockholm", "localityName": "Kista", "organizationName": "Fricsson", "organizationalinitName": "RCS", "commonName": "testCA", "emailAddress": "andreas.toyra@ericsson.com"]	['sample_C5.zip', '886648.img'
RSA	3072 PGP key	FALSE	FALSE	'BEGIN PGP PUBLIC KEY BLOCK		2027-03-15T10:30:06			['sample_C5.zip', '886648.img'
RSA	4096 PEM	FALSE	FALSE	'BEGIN PUBLIC KEY		2022-10-07T00:33:37	TRUE	["countryName": "NO", "stateOrProvinceName": "Oslo", "organizationName": "Sis-keysenvers.net CA", "commonName": "sis-keysenvers.net CA"]	['sample_C5.zip', '886648.img'
RSA	2048 PGP key	FALSE	FALSE	'BEGIN PGP PUBLIC KEY BLOCK		2019-12-31705:00:37			['sample_C5.zip', '886648.img'
RSA	2048 PGP key	FALSE	FALSE	BEGIN PGP PUBLIC KEY BLOCK					['sample_C5.zip', '886648.img'



4	А	В	С
1	Email	File	Domain
2	bash-maintainers@gnu.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash']	gnu.org
	bug-diffutils@gnu.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/sdiff']	gnu.org
	ssh-ed25519-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh-keygen']	openssh.com
•	ecdsa-sha2-nistp384-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh-keygen']	openssh.com
5	tun@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
	hostkeys-00@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
3	ssh-ed25519-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
9	umac-128-etm@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
0	forwarded-streamlocal@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
1	ecdsa-sha2-nistp384-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
2	cancel-streamlocal-forward@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
3	procps@freelists.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/top.procps']	freelists.org
4	jseward@bzip.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libbz2.so.1.0.6']	bzip.org
5	tun@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
5	hostkeys-00@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
7	ssh-ed25519-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	umac-128-etm@openssh.com	['sample C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	forwarded-streamlocal@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	ecdsa-sha2-nistp384-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	cancel-streamlocal-forward@openssh.com	['sample_c5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	posix-rename@openssh.com	['sample_cs.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	SIG@openssh.com	['sample_cs.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	heinrichh@duesseldorf.de	['sample_c5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/gnupg/help.de.txt']	duesseldorf.de
	heinrichh@duesseldorf.de	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/gnupg/help.ja.txt']	duesseldorf.de
	vp@test.ru	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/gnupg/help.ru.txt']	test.ru
	heinrichh@duesseldorf.de	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/gnupg/help.txt']	duesseldorf.de
	bug-cpio@gnu.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'ds/snare/grupg/nep.txt']	gnu.org
	procps@freelists.org		
		['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/ps.procps']	freelists.org
	jseward@bzip.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/bzip2']	bzip.org
	bug-diffutils@gnu.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/cmp.diffutils']	gnu.org
	bug-diffutils@gnu.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/diff.diffutils']	gnu.org
	bug-diffutils@gnu.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/diff3']	gnu.org
	ssh-ed25519-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/gpg-agent']	openssh.com
	ecdsa-sha2-nistp384-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/gpg-agent']	openssh.com
	preferred-email-encoding@pgp.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/gpg2']	pgp.com
	heinrichh@duesseldorf.de	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/gpg2']	duesseldorf.de
	hmac-md5-96-etm@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
	zlib@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
	eow@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
	ftp@example.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libcurl.so.4.5.0']	example.com
	hmac-md5-96-etm@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	zlib@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	eow@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
	pb@handhelds.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/update-rc.d']	handhelds.org
5	aschorr@telemetry-investments.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/awk/have_mpfr.awk']	telemetry-investments.co
7	aschorr@telemetry-investments.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/awk/inplace.awk']	telemetry-investments.co
3	ajt@debian.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/services']	debian.org
1	hakan@erix.ericsson.se	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/otp/lib/tftp-1.0.1/src/tftp.erl']	ericsson.se

Figure 136: C5 Infoleak email addresses (Black Duck)

IP	IPv6	File
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
192.168.0.254	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
192.168.0.20	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/ping.iputils']
10.18.44.13	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/build-info']
10.18.44.13	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/build-info.sh']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/hosts']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
192.5.5.213	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
192.33.137.200	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
192.33.137.209	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
192.33.137.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
192.33.137.250	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/Imt.sh']
0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/Imt.sh']
169.254.1.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
169.254.1.2	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
169.254.1.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
127.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
192.168.200.9	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
192.168.200.4	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
192.168.200.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
192.168.201.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
2001:4ca0:0:101::1	TRUE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
2001:4ca0:0:101:0:0:0:1	TRUE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
0.0.0.0	FALSE	['sample C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/ssh/sshd config']
0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/ssh/sshd_config_readonly']
1.2.3.4	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/ssl/openssl.cnf']
0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'lib64/libresolv-2.28.so']
10.11.12.13	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/autointegrate']
10.68.200.11	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/autointegrate']
141.1.2.3	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/autointegrate']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/nl_util']
10.1.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/etc/ipsec.conf']
10.2.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/etc/ipsec.conf']
192.168.0.2	FALSE	['sample_c5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/etc/ipsec.conf']
127.0.0.1	FALSE	['sample_C3.zip', 'BB6648.img', 'partition-0/initrd', 'n/stongswan/ib64/ipsec/libcharon.so.0.00']
0.0.0.0	FALSE	[sample_C3.zip', BB6648.img', 'partition-0/initrd', 'n/stongswan/lib64/ipsec/libstrongswan.so.0.0.0']
0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'n/stongswan/ib64/ipsec/nistrongswan.sto.co.i ]
255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'hi/suongswan/hoo4/ipsec/progriss/hostrongswan-suoke.:
FF02::1:2	TRUE	[sample_C5.2ip, BB6648.img, partition-0/initrd, sbin/arp.net-tools]
255.255.255.255		
	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/dhclient-script']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/epghd']
127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/htmd']
255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/ifcfg']

Figure 137: C5 Infoleak IP addresses	(Black Duck)
--------------------------------------	--------------

	А	В	С
1	Address	Vendor	File
2	00:11:22:33:44:55	CIMSYS Inc	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libies_sdk-50sm.so.2.12.1']
3	00:11:22:33:44:55	CIMSYS Inc	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libiesclient-50jm.so.2.12.1']
4			
	< > C5 in	nfoleak-macs +	

Figure 138: C5 Infoleak MAC addresses (Black Duck)

	А	В	С	D	E	F
1	Password	User	Algorithm	Salted	Hashed	File
2	ZPSwfmuzkO18o	sirpa	DES	FALSE	TRUE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/shadow']
3		root		FALSE	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/shadow']
4						
	< > C5 info	eak-passw	ords	+		

Figure 139: C5 Infoleak passwords (Black Duck)

.

A Url	B C
	File Domain
http://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash'] gnu.org
http://www.gnu.org/software/bash	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash'] gnu.org
http://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash'] gnu.org
https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils'] gnu.org
https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils'] gnu.org
https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils'] translationproject.o
https://www.gnu.org/software/coreu	
https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils'] gnu.org
0 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils'] gnu.org
1 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils'] translationproject.o
2 https://www.gnu.org/software/coreu	ls ['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils'] gnu.org
3 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils'] gnu.org
4 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils'] gnu.org
5 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils'] translationproject.o
6 https://www.gnu.org/software/coreu	
7 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils'] gnu.org
8 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils'] gnu.org
9 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils'] translationproject.o
0 https://www.gnu.org/software/coreu	
1 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils'] gnu.org
2 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils'] gnu.org
3 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils'] translationproject.o
4 https://www.gnu.org/software/coreu	
5 http://gnu.org/licenses/gpl.html	
1.1.0 0 10	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cpio.cpio'] gnu.org
6 http://www.gnu.org/software/cpio	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cpio.cpio'] gnu.org
7 http://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cpio.cpio'] gnu.org
8 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils'] gnu.org
9 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils'] gnu.org
0 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils'] translationproject.o
1 https://www.gnu.org/software/coreu	
2 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils'] gnu.org
3 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils'] gnu.org
4 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils'] translationproject.o
5 https://www.gnu.org/software/coreu	ls ['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils'] gnu.org
6 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils'] gnu.org
7 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils'] gnu.org
8 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils'] translationproject.o
9 https://www.gnu.org/software/coreu	ls ['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils'] gnu.org
0 https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils'] gnu.org
1 https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils'] gnu.org
2 https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils'] translationproject.o
3 https://www.gnu.org/software/coreu	
4 http://gnu.org/licenses/gpl.html	['sample_csizp', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep'] gnu.org
5 http://www.gnu.org/software/grep	['sample_c5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep'] gnu.org
6 http://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep'] gnu.org
7 http://git.sv.gnu.org/cgit/grep.git/tre	
8 https://www.gnu.org/licenses/gpl.ht	
1 0 0	
9 https://www.gnu.org/licenses/gpl.html	I ['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/gzip.gzip'] gnu.org

Figure 140: C5 Infoleak URLs (Black Duck)

Version 4.4.23 4.4.23 9.11.4 9.11.4 9.11.4 9.11.4	5.2.15 9.18.17	CVE-2019-18276 CVE-2022-3715	Matching type Exact match Exact match	CVSS CVE publication date 3.8 2019-11-29T14:52:13Z	Object compilation date 2020-02-02T05:06:07Z	Object bash.bash	Object full path	Object SHA1	7.8	CVSS vect CVSS vector (v3) AV:L/AC:L/PR:N/UEN/S:U/C:H/I:H/A:H/E:F/BLO/F
4.4.23 9.11.4 9.11.4 9.11.4	5.2.15 9.18.17	CVE-2022-3715					sample_C5.zip:886648.img:partition-0/initrd:bin/bash.bash	6e6b787521c26c016a832a000832343634986486		
9.11.4 9.11.4 9.11.4	9.18.17			3 2023-01-06T12:22:07Z	2020-02-02105:06:072	hash hash	sample_C5.zip:886648.img:partition-0/initrd:bin/bash.bash	6e6b783521c26c016a832a000832343634986485	5.1	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:P/RL:W/R
9.11.4 9.11.4		CVE-2020-8625	Exact match	5 2021-02-19T16:26:05Z	2020-02-02105:14:432	libbind9.so.160.0.8	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa98591224340af647052edf210b5	7.1	AV:N/AC:H/PR:N/UEN/S:U/C:H/EH/A:H/E:U/RLO
9.11.4		CVE-2020-8625	Exact match	5 2021-02-19T16:26:05Z	2020-02-02105:14:432	libisc.so.169.0.3	sample_C5.zip:886648.imgpartition-0/initrd:usr/lib64/libisc.so.169.0.3	a9856d4b06a9bd4071a82270acc2940095f75c63	7.1	AV:N/AC:H/PR:N/UEN/S:U/C:H/EH/A:H/E:U/REO
		CVE-2020-8625	Exact match	5 2021-02-19716:26:052	2020-02-02105:14:432	libisocfg.so.160.2.1	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libiscofg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	7.1	AV:N/AC:H/PR:N/UEN/S:U/C:H/EH/A:H/E:U/REO
		CVE-2018-5744	Exact match	4.7 2019-05-08T10:19:45Z	2020-02-02105:14:432	libbind9.so.160.0.8	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa98591224340af647052edf210b5	5.7	AV:N/ACL/PR:N/UI:N/S:U/CL/I:N/A:L/E:U/RL:O/R
9.11.4		CVE-2018-5744	Exact match	4.7 2019-05-08T10:19:45Z	2020-02-02T05:14:432	libisc.so.169.0.3	sample C5.zip:886648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a9856d4b06a9bd4071a82270acc2940095f75c63	5.7	AV:N/ACI/PR:N/UI:N/SIJ/CI/I:N/AII/EIJ/RLO/R
9.11.4		CVE-2018-5744	Exact match	4.7 2019-05-08710:19:452	2020-02-02105:14:432	libiscofg.so.160.2.1	sample_C5.zip/886648.img:partition-0/initrd:usr/lib64/libiscofe.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	5.7	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/E:U/RL:O/R
9.11.4		CVE-2020-8617	Exact match	4.1 2020-05-21713:21:072	2020-02-02105:14:432	libbind9.so.160.0.8	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa98591224340af647052edf210b5	7	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E/F/RI:O/
9.11.4		CVE-2020-8617	Exact match	4.1 2020-05-21713:21:072	2020-02-02T05:14:432	libisc so 169.0.3	sample C5.zip:886648.img.partition-0/initrdusr/lib64/libisc.sp.169.0.3	a9856d4b06a9bd4071a82270acc2940095f75c63	7	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E/F/RLO
									7	AV:N/AC:L/PR:N/UI:N/S:U/C:N/EN/A:H/E/F/RL:O/
										AV:N/AC:H/PR:N/U:N/S:U/C:H/I:H/A:H/E:U/RLO
										AV:N/AC:H/PR:N/UEN/S:U/C:H/EH/A:H/EU/RED
										AV:N/AC:H/PR:N/U:N/S:U/C:H/IH/A:H/E:U/RL:O
										AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/
										AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/
										AV:N/ACL/PR:N/U:N/S:C/C:N/U:N/A:H/EU/REG
			erer:							AV:N/ACI/PR:N/UI:N/SIJ/C:N/I:N/A:H/EU/RL:O
										AV:N/ACL/PR:N/UEN/SU/CN/IN/ACH/EU/RLO
										AV:N/ACL/PR:N/U:N/SU/C:N/IN/A:H/EU/RLO
										AV:N/ACI/PR:N/UI:N/SIJ/CIN/CIN/ACH/EU/REG AV:N/ACI/PR:N/UI:N/SIJ/C:N/I:N/ACH/EU/REG
										AV:N/ACI/PR:N/UI:N/SIJ/C:N/UR/A:H/EU/RLC
										AV:N/ACL/PR:N/UI:N/SU/C:N/UN/A:H/EU/RLC
										AV:N/ACL/PR:N/UEN/SU/C:N/IN/A:H/EU/RLC AV:N/ACL/PR:N/UEN/SU/C:N/IN/A:H/EU/RLC
										AV:N/ACI/PR:N/UEN/SU/C:N/UN/A:H/EU/BLC AV:N/ACI/PR:N/UEN/SU/C:N/UN/A:H/EU/BLC
										AV:N/ACL/PR:N/UEN/SU/C:N/UN/A:H/EU/RLC
										AV:N/ACI/PR:N/UEN/SU/CN/IN/A:H/EU/REC AV:N/ACI/PR:N/UEN/SU/CN/IN/A:H/EU/REC
										AV:N/ACL/PR:N/UEN/SU/C:N/UN/A:H/EU/RLC AV:N/ACL/PR:N/UEN/SU/C:N/UN/A:H/EU/RLC
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/EN/A:H/E:U/RL:C
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:C
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/EN/A:H/E:U/RL:C
										AV:N/ACI/PR:N/UI:N/SIJ/C:N/I:N/A:H/EIJ/RLIO
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/EN/A:H/E:U/RL:O
										AV:N/ACI/PR:N/UI:N/SIJ/C:N/IN/A:H/EU/RL:O
										AV:N/ACI/PR:N/UI:N/S:U/C:N/I:N/A:H/EU/RLC
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/UN/A:H/E:U/RL:C
										AV:N/ACI/PR:N/UI:N/S:U/C:N/IN/A:H/EU/RLC
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:C
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/EIU/RL:C
										AV:N/ACIL/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O
										AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:C
9.11.4			Exact match	3.7 2020-08-21711:03:232	2020-02-02105:14:432					AV:N/AC:L/PR:N/UI:N/S:U/C:N/EN/A:H/E/U/RL:C
9.11.4										AV:N/ACI/PR:N/UI:N/SIU/CIN/IIN/AIH/EIU/RLIC
9.11.4			Exact match	3.7 2019-05-14T11:02:26Z	2020-02-02105:14:432					AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:C
9.11.4			Exact match	3.7 2019-05-14T11:02:26Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a9856d4b06a9bd4071a82270atc2940095f75c63	6.5	AV:N/ACI/PR:N/UI:N/SIJ/C:H/I:N/A:N/EIJ/RL:O
9.11.4			Exact match	3.7 2019-05-14T11:02:26Z	2020-02-02105:14:432	libiscofg.so.160.2.1	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/ACIL/PR:N/UI:N/SJU/C:H/I:N/A:N/EJU/RL:O
9.11.4	9.18.17	CVE-2018-5743	Exact match	3.7 2019-04-29T13:57:32Z	2020-02-02105:14:432	libbind9.so.160.0.8	sample_C5.zip:886648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa98591224340af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/EN/A:H/E:U/RL:O
	9.11.4 9.11.4	8.1.1.4         9.1.1.4         9.1.1.7           8.1.1.4         9.1.1.7         9.1.1.7           8.1.1.4         9.1.1.7         9.1.1.7           8.1.1.4         9.1.1.7         9.1.1.7           8.1.1.4         9.1.1.7         9.1.1.7           8.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7         9.1.1.7           9.1.1.4         9.1.1.7 <td< td=""><td>31.41         31.81         0.81.07         0.75.07.001           31.81         0.81.07         0.75.07.001         0.75.07.001           31.81         1.81.07         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         0.81.0</td><td>State         State         <th< td=""><td>11.11         11.12         0.12         0.02           11.11         11.12         0.02         <t< td=""><td>11.1         <th< td=""><td>N1.14         N1.14         <th< td=""><td>11.1         <th< td=""><td>11.1         11.1.1</td></th<></td></th<></td></th<></td></t<><td>11.1         <th< td=""></th<></td></td></th<></td></td<>	31.41         31.81         0.81.07         0.75.07.001           31.81         0.81.07         0.75.07.001         0.75.07.001           31.81         1.81.07         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         1.81.17         0.75.07.001         0.75.07.001           31.81         0.81.0	State         State <th< td=""><td>11.11         11.12         0.12         0.02           11.11         11.12         0.02         <t< td=""><td>11.1         <th< td=""><td>N1.14         N1.14         <th< td=""><td>11.1         <th< td=""><td>11.1         11.1.1</td></th<></td></th<></td></th<></td></t<><td>11.1         <th< td=""></th<></td></td></th<>	11.11         11.12         0.12         0.02           11.11         11.12         0.02 <t< td=""><td>11.1         <th< td=""><td>N1.14         N1.14         <th< td=""><td>11.1         <th< td=""><td>11.1         11.1.1</td></th<></td></th<></td></th<></td></t<> <td>11.1         <th< td=""></th<></td>	11.1         11.1 <th< td=""><td>N1.14         N1.14         <th< td=""><td>11.1         <th< td=""><td>11.1         11.1.1</td></th<></td></th<></td></th<>	N1.14         N1.14 <th< td=""><td>11.1         <th< td=""><td>11.1         11.1.1</td></th<></td></th<>	11.1         11.1 <th< td=""><td>11.1         11.1.1</td></th<>	11.1         11.1.1	11.1         11.1 <th< td=""></th<>

Figure 141: C5 CVEs (Black Duck)

# Sample C5 Code Sentry Scan Report Excerpts

$\equiv$	<sup>I</sup> CODESentry	TM			
	+ NEW SCAN				
			N-DAY FINDINGS		ZERO-DAY FINDINGS
<b>JII</b> D	Dashboard		Security Score		Security Score
BB s	Summary		N/A Artifact 0 Scan Quality		N/A <sup>Artifact</sup> N/A <sup>Scan</sup> Security N/A <sup>Quality</sup>
ر م			0 Findings		0 Findings
	DevOps	$\odot$			
🛄 N			None Discovered		None Discovered
(	<b>С</b> , А1				
			Unescioned None Low Medium High Critical		Low Medium High Critical
(	©, A2				
(	🕼 АЗ	N	G Evaluation > C5_zipped > sample_C5.zip:	Scan Done, Sca	an Depth: Shallow

Figure 142: C5 Scan Overview (Code Sentry)



There were no components discovered.

Figure 143: C5 N-day findings (Code Sentry)



**N-Day Findings** 

Findings for sample\_C5.zip

Scan Depth: Shallow MD5: 7fcd7b01ee75dd1552f68d0e2a38d4be Number of Vulnerabilities: 0

### Figure 144: C5 Vulnerabilities (Code Sentry)

#### GRAMMATECH

<sup>I</sup>CODESentry<sup>-</sup>

Zero-Day Findings

Findings for sample\_C5.zip

Scan Depth: Shallow MD5: 7fcd7b01ee75dd1552f68d0e2a38d4be

Top 25 CWE Findings

Rank	ID	Name	Instances
1	CWE:787	Out-of-bounds Write	-
2	CWE:79	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	-
3	CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0
4	CWE:20	Improper Input Validation	-
5	CWE:125	Out-of-bounds Read	-
6	CWE:78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0
7	CWE:416	Use After Free	0
8	CWE:22	Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")	-
9	CWE:352	Cross-Site Request Forgery (CSRF)	-
10	CWE:434	Unrestricted Upload of File with Dangerous Type	-
11	CWE:476	NULL Pointer Dereference	-
12	CWE:502	Deserialization of Untrusted Data	-
13	CWE:190	Integer Overflow or Wraparound	-
14	CWE:287	Improper Authentication	-
15	CWE:798	Use of Hard-coded Credentials	0
16	CWE:862	Missing Authorization	-
17	CWE:77	Improper Neutralization of Special Elements used in a Command ("Command Injection")	-
18	CWE:306	Missing Authentication for Critical Function	-
19	CWE:119	Improper Restriction of Operations within the Bounds of a Memory Buffer	0
20	CWE:276	Incorrect Default Permissions	-
21	CWE:918	Server-Side Request Forgery	-
22	CWE:362	Concurrent Execution using Shared Resource with Improper Synchronization ("Race Condition")	-
23	CWE:400	Uncontrolled Resource Consumption	-
24	CWE:611	Improper Restriction of XML External Entity Reference	-
25	CWE:94	Improper Control of Generation of Code ("Code Injection")	-

#### All Other CWE Findings (Excluding Top 25 CWEs)

Severity	Score	CWE ID	Name	Instances
None				

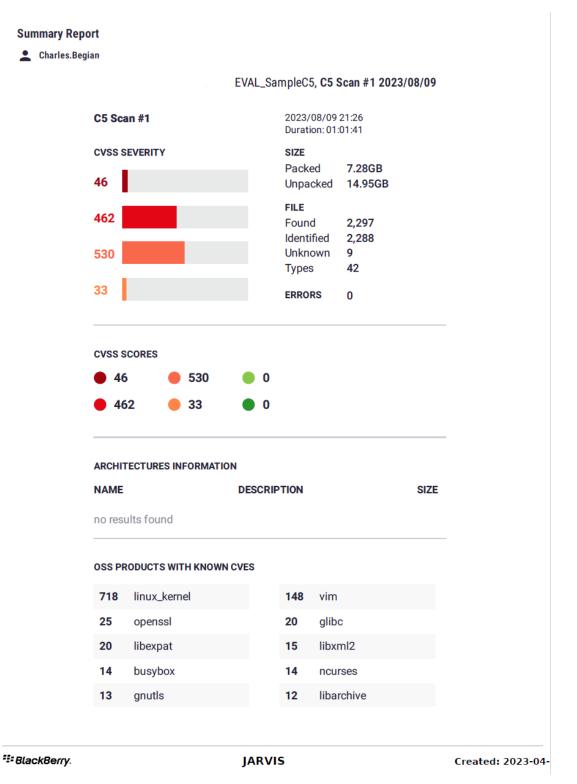
www.grammatech.com

Page 4 / 11

CodeSentry is a registered trademark of GrammaTech, Inc.

Figure 145: C5 Zero-day findings (Code Sentry)

# <sup>I</sup>CODESentry<sup>-</sup>

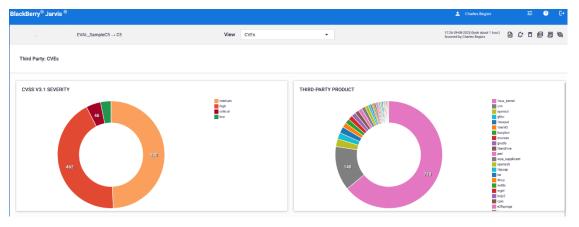


# Sample C5 Jarvis Scan Report Excerpts

Figure 146: C5 Scan Overview (Jarvis)

:Berry® Jarvis ®				
EVAL_SampleC5 - C5		View Classified Strings		17.35 09 10 2020 (stock about 1 hour) Scorrently Charles Begins
formation Leakage: Classified Strings (BETA)				
TRING CATEGORY		Driverwine Laskage	STRING TYPE	Saras linguit
		E Sank Galy E Sank Galy E Sank Galy Read	200	3.000
8,975				
FILE INFO + FILE PATH	STRING TYPE	CATEGORY	STRING	PULL STRING
TILE INTO + FILE PATH	STRING TYPE Hex Encoded	CATEGORY Encoded	STRING STRING Statistics of the state of the	PAL STEING
NLE INFO + FILE PATH Isampla.CS ang				060050555555555556666666666666666666666
ILE AVO - FILE PATH sample_CS ang	Hex Encoded	Encoded		
YILE INFO + FILE PATH MangleLCSSing Inample_CSsing	Hex Encoded	Encoded Code Quality		ыколоталосола колотория солотория солотория и солотория солотория солотория солотория солотория солотория солот Солотория солотория с WMT-USS
NLE MO - NLE PATH Annahu, CSing Inangk, CSing Annahu, CSing Annahu, CSing Annahu, CSin	Hex Encoded TODO Source file path Source file path Source file path	Encoded Code Quality Information Leakage	atomantenanaennennennennennen Wif PL:s	алалалаалаалаалаалаалаалаалаалаалаалаал
YILE M <sup>I</sup> CH + FILE MATH Amminik. CSing Sample, CSing Amminik, CSing Sample, CSing Samp	Hex Encoded TODO Source file path Source file path	Encoded Code Quality Information Loskage Information Loskage	uningenerativenerativenerativenerativenerativenerativenerativenerativenerativenerativenerativenerativenerativen Not Not	насоллански половили половили 1979—295 17721 Б.К.С.
TLE MC+TLE PATH anaple.25ing anaple.25ing anaple.25ing anaple.25ing anaple.25ing anaple.25ing anaple.25ing anaple.25ing anaple.25ing/anaple.25ing/25i2/25i2/25i2/25i2/25i2/25i2/25i2/25i	Hex Encoded TODO Source file path Source file path Source file path	Encoded Code Quality Information Laskage Information Laskage	ала почила почила на почила почила почила Ved //C.e. //Funu/spycelle.b.h	алалалаалаалаалаалаалаалаалаалаалаалаал
ALLE NO + ALLE PACH Hample, C.S. Ting Hample, C.S. Ting Hample, C.S. Ting Journal Hample, C.S. Ting Journal (J. C. Margueri E. J. M. College Hample, C.S. Ting Journal (J. C. Margueri E. J. M. College Hample, C.S. Ting Journal (J. M. Ting Journal J. J. College Hample, C.S. Ting Journal (J. Ting Journal J. J. College Hample, C.S. Ting Journal (J. M. Ting Journal J. J. College Hample, C.S. Ting Journal (J. M. Ting Journal J. J. College Hample, C.S. Ting Journal (J. Strange) Hample (J. S. Ting Journal (J. Strange) Hample (J. S. Ting Journal (J. Strange) Hample (J. S. Ting Journal (J. Strange) Hample (	Her Encoded TODO Source file path Source file path Source file path	Encoded Code Quality Information Leakage Information Leakage Information Leakage Information Leakage	anterinanterinanterinanterinanterinanterinanterinanterinanterinanterinanterinanterinanterinanterinanterinanteri Price Price Price Price Price Price Pr	иссологологологологологологологологологол
TLE INV + FLE PATH Sample, CS Ing Sample, CS Ing Sample, CS Ing Sample, CS Ing Sample, CS Ing Sample, CS Ing Sample	Hex Encoded TODO Source file path Source file path Source file path Source file path TODO	Encoded Code Quality Information Leakage Information Leakage Information Leakage Information Leakage Code Quality	anarima marina marina marina marina Na Ita Ita Itali Mautopeda ti Aduja matukan Bug	utanatanatanatanatanatanatanatanatanatan
HLENG - FILE PATH HELENG - TILE	Here Encoded TODO Source Repath Source Repath Source Repath Source Repath TODO Source Repath	Encoded Code Gually Information Londope Man mation Londope Man mation Londop Manager Code Gually Information Landop	estatuares menores anternational ME ME /AC /Advantscore. Majoressarianistos.	μασοποτοιοποιοποιοποιοποιοποιοποιοποιοποιοπ
All and o . FLE ANTA           Anargia L. Shing           Sample, L. Shing Sample, L. Shing Sample, Shing Sample, Shing Sample, L. Shing Sample, Shin	Here Frooded TODO Source He path Source He path Source He path Source He path TODO Source He path Source He path	Treaded Code Quality Information Lankage Information Lankage Information Lankage Code Quality Information Lankage Information Lankage	entrementaria entrementaria entrementaria Vel Kes Kespecifico entrementaria Mali contractora e Addorentariatoria e Addorentariatoria e	editorial and a second a seco
NLL WO - JYLE WAT Warriel, C.Sing Warriel, C.Sing Sangle, C.Sing Sangle, C.Sing Sangle, C.Sing Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , <i>90</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>122</i> , 500, 445 Sangle, C.Sing-Spatian, <i>Nationage</i> , <i>124</i> , 500, 445 Sangle, Sangle, Sangle, <i>144</i> , 500, 445 Sangle, Sangle, <i>144</i> , 500, 445 Sangle, <i>144</i> , 510, 510, 510, 510, 510, 510, 510, 510	Her Encoded TODO Source IR-path Source IR-path Source IR-path TODO Source IR-path Source IR-path Source IR-path Source IR-path	Encoded Coale Gually Information Longon Information Longon Information Longon Information Longon Coale Gually Information Longon Information Longon Information Longon	антинания налична на на Ис Ис Ис Искородско И Искородско Искородско Искородско И Искородско Искородско И Искородско И И И И И И И И И И И И И И И И И И И	VICANALIZATIONNE CONTRACTANTICA CONT
LE NO + FLE PATH           Sample, C.Sing           Sample, C.Singupation, Mannagidze, P.DOCM#95263.0000181           Sample, C.Singupation, Mannagidze, P.DOCM#95262.0000181           Sample, C.Singupation, Mannagidze, P.COCM#95262.0000181           Sample, C.Singupation, Mannagidze, P.COCM#95262.0000181 <td>Here Encoded TODO Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath</td> <td>Transfeld Coate Cuality Information a subage Information a subage Information a subage Information a subage Coate Cuality Information a subage Information a subage Information a subage</td> <td>enternamental and a second and</td> <td>editorial and a second and a se</td>	Here Encoded TODO Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath Source (Ropath	Transfeld Coate Cuality Information a subage Information a subage Information a subage Information a subage Coate Cuality Information a subage Information a subage Information a subage	enternamental and a second and	editorial and a second and a se
HLING of LENTH  Variang LCS Ing  Anange CS Ing Anange CS Ing  Anange CS Ing Anange CS Ing  Anange CS Ing Anange CS Ing Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing  Anange CS Ing Anange CS Ing Anange CS Ing  Anange CS	Heir Encoded TODO Source Heip anh Source Heip anh Source Heip anh TODO Source Heip anh Source Heip anh Source Heip anh Source Heip anh	Encoded Coale Gually Information Landge Information Landge Information Landge Information Landge Information Landge Information Landge Information Landge Information Landge Information Landge	Hammennen minnen minnen Ka Ka Kas Kaspenden Kadonen jone a Kadonen jone Ka Kadonen jone Ka Kadonen jone Ka	deconstructions deconstructions deconstructions     Wird-aG     Wird-aG     Vird-aG     Vird-aG     Vird-aG     vird-aditional deconstruction deconstruction deconstruction     advalationation and addition deconstruction     advalationation biological     advalationationation biological     advalationationation biological     advalationationation     advalationationationation     advalationationationation     advalationationationation     advalationationationation     advalationationationationationation     advalationationationationation     advalationationationationationationation     advalationationationationationationationation
ILL INFO - FLE PATH           Ananyla, C.Shog	Her Droded TODO Source Reputh Source Reputh Source Reputh Source Reputh Source Reputh Source Reputh Source Reputh Source Reputh Source Reputh	Transfeld Coath Caelly Information Landger Information Landger Information Landger Information Landger Coath Caelly Information Landger Information Landger Information Landger Information Landger Information Landger	enternational and a second and	essential essent
Last     Kurno - ALE MAX     Anarqie A.Sting     Anarque A.St	Hen Encoded TODO Source Heguth Source Heguth	Encoded Coarlo Cuality Information Landage Information Landage Information Landage Order Cuality Information Landage Information Landage Information Landage Information Landage Information Landage Information Landage	Hammennennennennennennen Wei Kei Kass Anservenke Adorenstränder Addreserstränder Addreserstränder Addreserstränder Addreserstränder Addreserstränder	

Figure 147: C5 Information leakage (Jarvis)



## Figure 148: CVSS Severity Report (Jarvis)

ackBerry <sup>®</sup> Ja	rvis <sup>®</sup>										
Scan Results	Charles.Begian@ 🔻	EVAL_Sa	mpleC5 -								
COMPONENT	\$ NAME	¢ DATE	¢ CRITICAL	≑ HIGH	\$ MEDIUM	\$ LOW		UNPACKED SIZE	IDENTIFIED	¢ FOUND	\$ TYPES
EVAL_Sampl	C5	2023/08/09	46	462	530	33	7.28GB	14.95GB	2288	2297	42

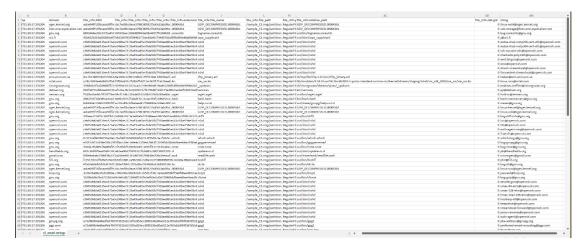
Figure 149: C5 CVE Summary by Severity (Jarvis)

			D																	
			file_info.file_name																	
2023-08-07	3 300	obe690:7337da	e sks-keyservers.netCA.pem	/sample_C5.img/partit	PEM_CERTIFICATE	TRUE	sks-keyservers.net CA	NO	sks-keyservers.net CA	202210070033372	201210090033372	FALSE	4,090	5	6 TRUE	sha1WithRSAEncryption	sks-keyservers.net CA	NO	sks-keyservers.net CA	
	) d'artificate + : +																			

Figure 150: C5 Certificates Report (Jarvis)

A		£	D £		0	R I	1	К.	L M	N.	0	Q	5	U V W	X V	// /# ·	AA z	4 ×	AL.
affected_versions	certain	components	OVE-OVELY OVE-OVEL			ve.cvss.v.cve.cvss.			4.0435.V (VE.0455.V		v cve.cvss.v3L vector	cve.name			pe cve refercesclu	olve, exclusi-			
[1.16.0, 1.34.0]	TRUE	busybox	1.9 low	FALSE	AV1./ACIN	5.5 medium	TRUE	CV55:3.0/.	5.5 medium	FALSE	CV55/3.1/AV1/AC1/PR1/UIIN/SIU/CIN/IIN/AIH	CVE-2021-42376	11/15/2021	4/25/2023 https://nvd.nist.gov/v CWE-476	https://jt null	rull	/sample_ >= 1.	34.0 busybo	4 125.2
[1.18.0, 1.33.1]	TRUE	busybox	6.5 medium	FALSE	AV:N/AC1	7.2 high	TRUE	CV55:3.0/-	7.2 high	FALSE	CV55:3.1/AV:N/ACIJ/PR:H/UEN/S:U/C:H/EH/A:H	CVE-2021-42384	11/15/2021	4/15/2023 https://nvd.nist.gov/v CWE-416	https://jt null	null	/sample_>1.3	3.1 busybo	4 1.29.7
<8.44	TRUE	libptre	5 medium	FALSE	AV/N/ACI	5.3 medium	TRUE	CV55:3.0/.	5.3 medium	FALSE	CV55:3.1/AV:N/ACIU/PR:N/UEN/S:U/CIN/EN/ASI	CVE-2020-14155	6/15/2020	12/5/2022 https://nvd.nist.gov/v CWE-190	https://b null	null	/sample_ >= 8.	44 ppre	1
< 8.43	TRUE	libpore	4.3 medium	FALSE	AV:N/AC1	7.5 high	TRUE	CV55:3.0/.	7.5 high	TALSE	CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/C:N/EN/APR	CVE-2019-20838	6/15/2020	5/22/2021 https://nvd.nist.gov/v CWE-125	https://b null	null	/sample_>=8.	45 pore	14
<r2.5< td=""><td>TRUE</td><td>wps cli</td><td>3.3 low</td><td>FALSE</td><td>AV:A/ACI</td><td>0.5 medium</td><td>TRUE</td><td>CV55:3.0/</td><td>6.5 medium</td><td>TALSE</td><td>CV55:3.1/AV-A/AC:L/PR:N/UEN/S:U/C:N/EN/A:H</td><td>CVE-2019-16275</td><td>9/12/2019</td><td>8/24/2020 https://med.ntst.gov/v CWE-346</td><td>mult</td><td>null</td><td>/semple &gt;2.5</td><td></td><td>loc .</td></r2.5<>	TRUE	wps cli	3.3 low	FALSE	AV:A/ACI	0.5 medium	TRUE	CV55:3.0/	6.5 medium	TALSE	CV55:3.1/AV-A/AC:L/PR:N/UEN/S:U/C:N/EN/A:H	CVE-2019-16275	9/12/2019	8/24/2020 https://med.ntst.gov/v CWE-346	mult	null	/semple >2.5		loc .
4.1-esy [4.4.0, 4.4.2]	TRUE	dhepd	3.3 low	FALSE	AV:A/ACI	7.4 high	TRUE	CV55:3.05	7.4 high	FALSE	CV55:3.1/AV-A/ACIJPR:N/UIN/S:C/CN/I:N/AH	CVE-2021-25217	5/26/2021	5/3/2023 https://mid.nist.gov/v CWE-119	https://k mull	null	/sample (>4.4	1.2 dhop	4.4.1
1.0.0, 4.1-esv], [4.2.0, 4.4.3]	TRUE	dhend	6.1 medium	TRUE	AV:A/AC:I	6.5 medium	TRUE	CV55:3.8/-	6.5 medium	FALSE	CV55:3.1/AV:A/AC://PR:N/UDN/S:U/C:N/I:N/A:H	CVE-2022-2929	30/7/2022	5/3/2023 https://nvd.nist.gov/v CWE-770	https://k mull	mall	/sample (>4.4	anth £1	4.4.1
L1-ety (440, 44.1)	TRUE	dhead	6.1 medium	TRUE	AV:A/AC:I	6.5 medium	TRUE	CV55:3.0/.	6.5 medium		CV55:3.1/AV:a/AC:JPR:N/UEN/S:U/C:N/EN/A:H		10/7/2022	5/3/2023 https://myd.nist.acv/v.CWF-476	https://k_mull	mult	/sample 1>4.6		441
1868 87.11	TRUE	libenutis	7.5 high	FALSE	AV:N/ACI	9.8 critical	TRUE	CV55:3.05	9.8 critical	14/15	CV55/3.1/AV/N/ACIL/PRIN/UEN/S/U/CHI/LH/AH	CVE-2021-20231	3/12/2021	6/1/2021 https://mvd.nist.gov/v.CWE-416	mult	null	/sample (1+3	7.1 muth	3.6.4
3.6.12		liberatis	4.3 medium			5.9 medium	TRUE	CV55:3.0/	5.9 medium		CVSS-3.1/AV:N/AC:H/PR:N/UEN/SU/C:H/EN/A/N		8/22/2018	2/13/2023 https://nvd.nist.gov/v CWE-385	https://ei.nu/l	itun	/sample (>= 3)		3.6.4
-3.6.4		Idenutis	3.3 low	FALSE		5.6 medium	TRUE	CV55:3.07	5.6 medium		CV5S:3.1/AV.P/ACH/PRL/ULN/S:C/CH/LL/A/N	CVE-2018-16868	12/3/2018	11/30/2022 https://nvd.nist.gov/v CWE-205	https://b null	null	/sample 1>3.6		3.6.4
w7.9		openab	4 medium			0.0 medium	TRUM	CV55.3.8/	6.8 medium		CV553 1/AV N/ACH/PEN/AEB/SU/CH/EH/A/N		1/31/2019	2/23/2023 https://wel.not.gov/v CWE-116	https://si mult	null	/sample > 2.9		
±7.9	TRUE		2.6 low	FALSE		5.3 medium	TRUE	CV55:3.0/	5.3 medium		CV55:3.1/AV:N/AC:H/PR:N/JER/S:U/C:N/EH/A:N		1/10/2019	2/23/2023 https://nvd.nist.gov/v CWE-863	https://gi null	mail	/sample >7.5		
6.2.6.0	TRUE	openish	4.4 medium			7 high	TRUE	CV55:3.0/	7 high		CV55-3.1/AV1/ACH/PR1/UEN/S:U/CH/EH/AH	CVE-2021-41617	9/26/2021	2/14/2023 https://wd.nist.apy/y NVD-CWE-Other		null	/sample >c 8.		
102.1024.[11.1.1.1.10	TRUE	Ideal	4.3 medium			5.9 medium	TRUE	CV55:3.0/.	5.9 medium		CV55:3.1/AV:N/AC:H/PR:N/UEN/S:U/CN/EN/A:H		12/0/2020	8/29/2022 https://wd.nist.gov/v CWE-476	Bun arty equin	null	/sample_ >= 1.		
1.0.2, 1.0.26, [1.1.0, 1.1.0]	TRUE	libesi	4.3 medium			3.7 kow	TRUE	CVSS3.0/	3.7 key		CVSS3.1/AVN/ACH/PRN/UN/SWC0/UN/A/N		5/10/2019	7/31/2021 https://www.nint.gov/v.cwe-476 7/31/2021 https://nvd.nist.gov/v.cwE-327, CWE-		null	/sample >11		
1.1.1.1.1.100. [3.0.0. 3.0.5]	TRUE	Hossi	5 medium			5.3 medium	TRUE	CV55:3.0/	5.3 medium		CV55/3.1/AV/N/AC/UPRIN/UE/N/S/U/CU/IN/A/N		7/5/2022	4/20/2023 https://www.not.gov/v.cwe-326	https://w null	flun	/sample_11.1		
1.0.2, 1.0.2rg), [1.1.1, 1.1.10]		Hossi	5.4 medium		AV/N/ACI	5.9 medium	TRUE	CV55:3.0/	5.9 medium		CV55.5.1/AV.N/ACH/PRIN/DDV5.0/CD/IN/A/N		2/8/2023	2/24/2021 https://wd.nist.gov/v.cvte-528 2/24/2021 https://wd.nist.gov/v.hvD.cwt-Othe	https://winull	null	/cample_ [1.1.		
1.0.2, 1.0.21g], [1.1.1, 1.1.1t] 1.0.2, 1.0.21b], [1.1.1, 1.1.1t]		Hossi	5.4 medium			5.9 medium 5.3 medium	TRUE	CV55:3.0/	5.3 medium		CV55:3.1/AV N/ACI/WEN/ULN/SU/CM/LI/A/N CV55:3.1/AV N/ACI/WEN/ULN/SU/CM/LI/A/N		3/26/2023	6/8/2023 https://wd.nid.gov/v.wvb.cwt-colo 6/8/2023 https://wd.nid.gov/v.CwE-235	https://winull	null			
						7.5 hath											/sample_ [1.1.		
1.0.2, 1.0.229}, [1.3.1, 1.1.34		Nosal	7.5 high	TRUE				CV55:3.0/	7.5 high		CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/C:N/UN/A:H		5/30/2023	6/9/2023 https://wed.nist.gov/v CWE-770	https://gi null	null	/sample_ [1.1.		
.0.2, 1.0.2zf), [1.1.1, 1.1.1p]		libsal	30 critical	FALSE		9.8 critical	TRUE	CV55:3.0/.	<b>9.8 critical</b>		CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/CH/RH/AH		6/23/2022	3/1/2023 https://wed.nist.gov/v CWE-78	https://gi mult	null	/sample_[1.1.		1.1.
2.29	TRUE	libpthread	5 medium			7.5 high			7.5 high		CVSS:3.1/AV:N/AC:L/PR:N/U:N/S:U/C:N/UN/ASH		2/26/2019	8/24/2020 https://wd.nist.gov/v CWE-674	https://s null	null	>2.2		
2.28	TRUE	libpthread	4.6 medium			5.3 medium	FALSE	CV55:3.0/	5.3 medium	TRUE	CV55:3.1/AV1/AC1/PR1/UEN/S1U/C1/EL/A1	CVE-2016-10739	1/21/2019	8/6/2019 https://nvd.nist.gov/v.CWE-20	https://s null	null	>2.2		
= 2.29	TRUE	libpthread	5 medium			7.5 high	FALSE		7.5 high		CV55:3.1/AV:N/AC:UPR:N/UEN/S:U/C:N/EN/APR		2/26/2019	11/5/2029 https://nvd.nist.gov/v CWE-674	https://li null	null	>2.2		
2.32	TRUE		6.4 medium			9.1 critical	TRUE		9.1 critical		CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/CH/I:N/A:H		7/22/2021	11/8/2022 https://nvd.nist.gov/v CWE-190	https://s null	null	242		
= 5.99.0		libricurses	7.5 high	FALSE		9.8 critical		CV\$5:3.0/-	9.8 critical		CV55:3.1/AV:N/AC:L/PR:N/UEN/5:U/CH/IEH/A:H		8/25/2019	8/29/2029 https://nvd.nist.gov/v CWE-119	https://runull	fun.	/sample_>5.9		
2.4.0			6.8 medium			7.3 high		CV55:3.0/-	2.3 high		CV55:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:L/EL/A/L	CVE-2013-0340	1/21/2014	2/13/2023 https://nvd.nist.gov/v CWE-611	nuit	null	/sample_t>=2.		
2.2.8		libespat	3 medium			7.5 high	TRUE	CV55:3.0/.	7.5 high		CV55:3.1/AV:N/AC:L/PR:N/UEN/S:U/C:N/EN/ASH		9/4/2019	7/28/2022 https://wed.nist.gov/v CWE-125, CWE-		null	/sampla_D=2.		
2.4.5	TRUE	libespat	7.5 high	FALSE	AV:N/AC:	9.8 critical	TRUE	CV55:3.0/.	9.5 critical	FALSE	CV55:3.1/AV:N/AC:L/PR:N/ULN/3:U/CH/I:H/A:H	CVT-2022-25315	2/18/2022	10/5/2022 https://nvd.nist.gov/v CWE-190	https://gi mull	mall	/sample_the2.	4.5 libespat	1 2.2.1
3.5.2	TRUE	liberthive	7.2 high	TRUE	AVS/ACS,	7.8 high	TRUE	CV55:3.0/i	7.8 high	FALSE	CV55:3.1/AV1/AC1/PR:N/U:R/S1J/C:H/EH/A:H	CVE-2021-23177	8/23/2022	12/3/2022 https://wwd.nist.gov/v CWE-59	https://b mult	nuti	/sample_ >= 3.	5.2 liberchi	10333
3.4.0	TRUE	libarchive	5 medium	FALSE	AV/N/AC1	7.5 high	TRUE	CV55:3.0/.	7.5 high	FALSE	CV55:3.1/AV:N/AC:UPR:N/UEN/S:U/C:N/EN/APR	CVE-2019-18408	10/24/2019	11/1/2019 https://wwd.nist.gov/v CWE-416	https://gi null	Iton	/sample_>=3.	4.0 libarchi	ve 3.3.3
3.3.0, 3.4.0]	TRUE	Nbarchive -	4.3 medium	FALSE	AV:N/AC1	6.5 medium	TRUE	CV55/3.0/-	6.5 medium	FALSE	CV55:3.1/AV:N/AC:L/PR:N/UER/S:U/C:N/EN/A:H	CVE-2018-100087	79 12/20/2018	11/6/2029 https://nvd.nist.gov/v CWE-476	https://gi null	Itun	/sample_ >= 3.	4.0 libarchi	ve 3.3.
< 5.11.11	TRUE	linus_kentel	4.9 medium	FALSE	AV1/AC1	5.5 medium	TRUE	CV55:3.0/.	5.5 medium	FALSE	CV55:3.1/AV1/AC1/PRL/UEN/SU/CIN/EN/AH	CVE-2021-29649	1/30/2021	4/5/2021 https://mvd.nist.gov/v CWE-401	https://c null	null	/sample_roo5.	12.11 linux le	tri 4.58
-4.8	TRUE	linux kernel	6.8 medium	FALSE	AV:R/AC1	7.7 high	FALSE	CV55:3.0/.	7.7 high	TRUE	CV55:3.1/AV:N/ACIJ/PR:L/UEN/S:C/C:N/EN/A:H	CVE-2018-100003	2/9/2018	10/15/2020 https://nvd.nist.gov/v CWE-20	https://p mult	null	/sample_C5.im	g/parlinux lo	4114.58
(5.15.13	TRUE	linux kernel	4.6 medium	TRUE	AV1/AC1	5.5 medium	TRUE	CV55:3.0/.	5.5 medium	FALSE	CV55:3.1/AV1/AC1/PR1/UEN/SU/CN/EN/A:H	CVE-2023-25006	3/1/2025	5/15/2023 https://nvd.nist.gov/v CWE-476	https://gi null	null	/sample_t>=5.	15.13 linux, lo	4114.33
5.13.4	TRUE	lines kernel	7.2 high	TALSE	AVS/ACS	7.8 high	T\$1,6	CV55:3.0/.	7.8 high	FALSE	CV55:3.1/AV1/AC1/PRL/URN/SU/CR/HH/AH	CVE-2021-18160	8/7/2021	1/1/2022 https://wei.nat.gov/v CWE-120	https://c mull	mult	/sample ()=5.	13.4 litrus k	ari 4.15
5.17.2	TRUE	linux kernel	4.6 medium	TRUE	AV1/AC1	5.5 medium	TRUE	cvss:a.n/.	5.5 medium	FALSE	CVSS-3.1/AV1/AC1/PR1/UEN/SU/CN/EN/AH	CVE-2023-22996	2/28/2023	3/6/2023 https://mvd.nist.gov/v CWE-772	https://c null	null	/sample tort5.	17.2 linux le	er: 4.13
2.12.5.4	TRUE	linux kernel	5.6 medium	FALSE	AVS/ACS	6.1 medium	TRUE	CV55-2.05	6.1 medium	121.62	CV55-3.1/AV1/AC1/PR1/UEN/S1J/CEN/EL/A:H	CVE-2019-19332	1/9/2020	2/12/2023 https://mvd.nist.agy/y CWE-787	https://w.mull	cull	Automale (>5.6	linux ke	err 6.18
(15.19.12	TRUE	linus kennel	d medium	TRUE	AVE/ACS	4.2 medium	TRUE	CV55:3.0/.	4.2 medium			CVE-2022-41849	9/30/2022	2/23/2023 https://med.nist.gov/v CWE-362, CWE-	Bun IV. rather 10	mult	/sample (>5.2	9.12 linux k	er: 4.18
-5.19	TRUE	linux kernel	6.5 medium	TRUE	AVIL/ACIL	6.7 medium	TRUE	CV55:3.0/.	67 medium	FALSE	CVSS-3.1/AV1/AC1/PR:H/ULN/S/U/CH/H/A/H	CVE-2023-2513	5/8/2023	5/15/2023 https://wwd.nist.gov/v CWE-416	https://gi null	null	/sample (>5.2	9 Neur Re	104.18
5.19		linux kernel	3.8 low		AVE/ACF	4.7 medium			4.7 medium		CV5S/3 1/AV1/ACH/PR1/ULN/SU/CN/LN/AH	CVE-2022-39188	9/2/2022	11/21/2022 https://nvd.nist.gov/v CWE-362	https://pi-null	Itun	/sample 1>+5.		
6.3			3.8 low		AV1/ACP	5.6 medium	TRUN	CV55-3.05	5.6 medium		CV553.1/AVL/ACH/PRL/ULN/EC/CH/IN/A/N	CVE-2023-1998	4/21/2023	5/3/2023 https://wwd.nist.gov/v CWE-203	https://k.mull	null	/sample t>=6.		
<5.2		linus, kernel	4.3 medium		AV1/AC1	3.5 medium	TRUE	CV55-3.0/	5.5 medium		CV55:3.1/AV1/AC1/PR1/ULN/SJU/CIN/EN/AH	CVE-2020-10720	3/3/2020	9/10/2030 https://wwd.nist.gov/v CWE-416	https://gi null	null	/sample ()=5.		
-3.9.0			3 medium			7.5 hath	TRUE	CV35:3.0/	7.5 high		CVSS:1.1/AV:N/ACL/PR:N/U:N/S:U/C:N/EN/A:N		10/13/2020	3/26/2021 https://nvd.nist.sov/v CWE-115	https://b mult	null	/sample (>5.5		
er 5.15	TRUE	linus kernel	4.9 medium			4.4 medium	TRUE	CV55:3.0/	4.4 medium		CVSE3.1/AV1/AC1/PEH/UI9/EU/CN/EN/AH	CVE-2023-4032	1/21/2022	1/28/2022 https://www.nite.gov/v.Cwt-115	https://b mult	ruli	/sample (>5.5		
G546	TRUE	linus kennel	2.1 low	FALSE		4.6 medium	TRUE	CVSS:3.0/	4.6 medium		CVSS3.1/AVP/AC1/PRIN/USN/SU/CH/IN/A/N	CVE-2019-19947	12/24/2019	11/9/2022 https://www.nin.gov/v.Cwc-439 11/9/2022 https://www.nint.gov/v.CwE-908	https://gi null	null	/sample (>5.4		
							TRUE		5.5 medium			CVE-2019-19947 CVE-2019-20095	12/30/2019			outi			
<5.1.6		linux_kernel	4.9 medium		AV1/AC1	5.5 medium		CVSS-3.8/	5.5 medium		CV55:3.1/AV1/AC1/PRI/URN/S1J/CIN/RN/A:H	CVE-2019-20050	12/40/2019	4/18/2022 https://wwd.nist.gov/v_CWE-401 10/4/2028 https://wwd.nist.gov/v_CWE-401	https://gi null	null	/sample_1>u.S.		
ci.com	1010	THE BARAN	a & moderne		Ann Inco.	a a modura	-ALCE	11110.00	a a strate on	1010	The second states and	- Inc 10 11015	azaronta.	HUNDER AND COMPANY AND AND A CALL AND	and the second	and the	resources a surge		Acre 28.1

Figure 151: C5 CVEs (Jarvis)



## Figure 152: C5 email addresses (Jarvis)

A	8	c	D	E	G		K	L		M	N	0	P	Q
@timestamp	tracked_pw	file_info.SHA3-512	file_info.	file_info.file_path	file_info.parent_path	gid	homedir	password	realname		scan_id	shell	uid	usemame
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d3 passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition_1/initrd/FiLE		34 /var/backups	•	backup		aedb8a1	/bin/sh		34 backup
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	tbcf2d1passwd	/sample_C5.img/partition_1/initrd/FILE/etc/passwd	/sample_C5.img/partition_1/initrd/FiLE		999 /var/run/dhcp	1			aedb6a1	/bin/false	9	199 dhcp
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8		/sample_C5.img/partition.1/initrd/FiLE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE	65,	534 /bin		sync		aedb8a1	/bin/sync		4 sync
2023-08-09721:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FILE		10 /vat/spool/uucp		uucp		aedb8al!	+/bin/sh		10 uucp
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8		/sample_C5.img/partition_1/initrd/FiLE/etc/passwd	/sample_C5.img/partition_1/initrd/FILE		33 /vat/www	•	www-data		aedb8a1			33 www-data
2023-08-09T21:30:17.391204		bb83794476930ed18695a60d18	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FiLE/etc/passed	/sample_C5.img/partition_1/initrd/FILE		13 /bin		proxy		aedb6a1	/bin/sh		13 proxy
2023-06-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition_1/initrd/FitE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE		41 /var/lib/gnats		Gnats Bug-Report	ting System (admin)	aedb8a15	/bin/sh		41 gnats
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition_1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FILE		998 /var/run/sshd	1			aedb8a1	/bin/false	9	198 sshd
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1 passwd	/sample_C5.img/partition_1/initrd/FILE/etc/passwd	/sample_C5.img/partition_1/initrd/FILE	65,	534 /nonexistent	•	nobody		aedb8a1	/bin/sh	65,5	i34 nobody
2023-08-09T21:30:17.391204	NO PASSWORD	bb83794476930ed18695a60d18	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition_1/initrd/FILE		0 /root		root		aedb8a15	/bin/sh		0 root
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1 passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE		1 /usr/sbin	•	daemon		aedb6a1	/bin/sh		1 daemon
2023-08-09721:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FiLE/etc/passwd	/sample_C5.img/partition.1/initrd/FILE		3 /dev		575		aedb8a1	/bin/sh		3 sys
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FILE		8 /var/mail		mail		acob6a1	/bin/sh		8 mail
2023-08-09T21:30:17.391204		bb83794476930ed18695a60d18	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FiLE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE		38 /var/list	•	Mailing List Mana	ger	aedb8a1	/bin/sh		38 161
2023-08-09721:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE		2 /bin		bin		aedb8a1	+/bin/sh		2 bin
2023-08-09721:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1 passwd	/sample_C5.img/partition_1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FILE		60 /ust/games		games		aedb6a1			5 games
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1 passwd	/sample_C5.img/partition_1/initrd/FiLE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE		12 /var/cache/man	•	man		aedb8a1	/bin/sh		6 man
2023-08-09T21:30:17.391204		bb83794476930ed18695a60d18	fbcf2d1 passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passed	/sample_C5.img/partition_1/initrd/FILE		7 /var/spool/lpd		lp		aedb8a1	/bin/sh		7 lp
2023-08-09721:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition_1/initrd/FitE/etc/passwd	/sample_C5.img/partition.1/initrd/FiLE		9 /var/spool/news		news		aedb8a1	/bin/sh		9 news
2023-08-09721:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition.1/initrd/FILE/etc/passwd	/sample_C5.img/partition.1/initrd/FILE		39 /vat/run/ircd	•	ircd		aedb8a1	/bin/sh		39 irc
2023-08-09T21:30:17.391204		bb83794476930ed18695a60df8	fbcf2d1passwd	/sample_C5.img/partition_1/initrd/FILE/etc/passwd	/sample_C5.img/partition_1/initrd/FILE		100 /home/sirpa	ZPSwfmuzkO18o	RCS system user		aedb8a19	/bin/sh	1,0	000 sirpa
c > c5 passwd-														

Figure 153: C5 Password File Analysis (Jarvis)

	8	U U E F I	K		M	AR.	Hi.	AK	AA.
					o.ttile_info.gtile_info.pa		netloc	string	
17.391204	893444ec92c37ctce457a74c187448b	41td32ee3028d8954L6etde4bt3ttc504bb9 logname.coreutik		ELF		Ling/partition.1/initrd/FILE		https://www.gnu.org/software/coreutils	
17.391204	bd51743509f79Mce1b37ccfb79270e	Laac93ole 8b2118adcab000b2(bed34147) cgdisk	/sample_C5.img/partition.1/initrd/FILF/ust/sbin/ogdisk	FLF	RegularFil/sample_CS	Ling/partition_1/inited/FILF	www.lbm.com	http://www.lbm.com/developerworks/linux/library/l-6kb-sector-disks	
17.391204	2606b20a52a8a177ba16e0f07bcd5ad	50x4e1871 71474c811: 2x4b381c1 75e1c9315 cpin.cpin	/sample_C5.img/partition.1/initrd/FiLE/bin/cpio.cpio	ELF	RegularFil/sample_C5	Ling/partition_1/initrd/FiLE	www.gnu.org	http://www.gru.org/saftware/cpio	
7.391204	3d7008b9a29a25790abee1d29dfeb20	3b4feb14549cbd6f665e1c56445bc7729971sed.sed	/sample_C5.img/partition.1/initrd/FILE/bin/sed.sed	ELE	RegularFil/sample_CS	.img/partition_1/initrd/FILE	www.gnu.org	http://www.gru.org/software/sed	
17.191204	7da4d2b00e82431ae311bb92321e618	731e3686(d1d83092) 55700c5dz 555e9b41(updatedb	/sample_C3.img/partition.1/initrd/FILE/usr/bin/updatedb	SHELL_S	CI RegularFil/sample_C5	Ling/partition_1/initrd/FiLE	www.gnu.org	http://www.gru.org/liconses	
17.391204	7a7d4aaca28f5abb8b1341f3aeab371	f605b8153 b9ded47o 5ae58b5a' 8df7aa2dE ericsson-icons.woff	/sample_C3.img/partition.1/initrd/FILE/rl/ServerRoot/htdocs/icons/erics:	TTE	RegularFil/sample_C5	Ling/partition_1/initrd/FILE	www.ericsson.com	https://www.ericsson.com	
7.991204	bb273c0fea5524a8cfea443befbdd96	d569c7fd8476bo700c064ba930cdcf70148dgawk	/sample_C3.img/partition.1/initrd/FILE/usr/bin/gawk	ELF	RegularFil/sample_C5	Umg/partition_1/initrd/FILE	www.gnu.org	https://www.gnu.org/software/gawk/manual/html_node/Bugs.html	
7.391204	14a46953d07c3565ae51a2e527802db	fof1bd40b 78400b2ct 17876ac6c 83fd44d3c Config.pm	/sample_C5.img/partition.1/initrd/FLE/usr/lib64/perl/5.24.4/Config.pm	PERL SC	CR RegularFil/sample C5	Ling/partition_1/initrd/FILE	perl5.git.perl.org	http://perl5.git.perl.org/perl.git/blob/HEAD:/Perting/Glossary	
7.391204	af3e2bc1d800d5e289a2bc897d94106	a139c7000 adoc3b9d: 13b7137b1 fa807aba3 grep, grep	/samale_CD/img/partition_1/initrd/FILE/bin/grep.grep	ELF	RegularFil/sample C5	Umg/partition_1/initrd/FILE	WWW.ENU.OR	http://www.gtu.org/software/grep	
7.292204	9d2bc0ceb079f23ff7be114ddc4c9fa	04o417d6) 335da033: 528b131bi b305a8da wget.wget	/semale C3.img/partition_1/initrd/FILE/usr/bin/wget.wget	LU	RegularFil/sample C5	Ling/partition_1/initid/Fita	www.gnu.org	http://www.gtu.org/licenses/gol.html	
.391204	(21c0x40e38440224ba0197991cb9879	c89f10ef7-3737actid£e7e73bb76ftccbfa1:wgetrc	/sample_CD.img/partition_1/initrd/FILE/etc/wgetrc	ASCIL	RegularFil/sample C5	ume/partition_1/initid/FILE	WWW.ENJ.OR	https://www.enu.org/software/weet/manual/weet.html#Startup.File	
/.292204	002253F3da905ce1ea1/f123f6a0/1f	6e6b/8/5/5/5dad4/b.3c3ao436F2d6022ccd bash.bash	/sample CS.mg/partition_1/initrd/FIG/bin/bash.bash	EUF .	RegularFil/sample CS	img/partition_1/mitrd/FILE	www.gou.org	http://www.gru.org/software/bash	
/.291204	1aab/2d425b175a9366663925b4c051	d44b/fe7j080de0ba/6c749ab7c4ae6d99c5ct_log_list.onf.dist	/sample C5/mg/partition_1/intrd/FRE/usr/hb64/ssl-1.1/ct log list.onf.de	ASCIL	RegularFil/sample C5	ime/partition_1/mitrd/FILE	www.cerbficate-transparency.org	www.certificate-transparency.org/known-logs	
191204	k9d4c810212451cf5427e5f1ff597fc	1366629f+bfd3409c4be478215;8beb1d39 openssl	/semple_C5.img/partition_1/initrd/FILE/ust/bin/openssl	ELF	RegularFil/sample CS	img/pertition_1/mitrd/FILE	ethers.isbber.org	http://etherx.iabber.org/streams	
291204	1512def9c380f1c2bda6e95c917d313	baa58a4ci;c16971e1Ec941c515a;d1500e8812ipiefo	/sample_C5.img/partition_1/initrd/FRE/usr/bin/zipinfo	ELF	RegularFil/sample CS	img/partition_1/inited/FILE	www.itfo-zip.org	http://www.info-zip.org/zip-bug.html	
101201	b1foe6d153644f351545c02405eb0e7	428x22x01502843de 87510e90.d49bd65fclibxml2.so.2.9.8	/semple_C5.img/partition_1/initrd/Titt/usr/lib64/libont2.so.2.9.8	EUT .	RegularFil/sample_CS	Ling/partition_1/initrd/TLE	relaing.org	http://relaxing.org/rs/structure/1.0	
		cbr7ed9br0ace3798(8093275dF613ab09ccG2IP_DECOMPRESSED.000043b1		ELF		imploartition.1/brimare		https://www.kemel.org/doc/html/latest/admin-quide/hw-vuln/mds.html	
111201		cbc7ed9bc0ace3798C8093275dF613ab09ccG2IP_DECOMPRESSED.000043b1		FIF	RegularFil/sample CS	Ling/partition.1/brimage	ware abit com tw	http://www.abit.com.tw	
391204		04aeb789i b13782730 6e8132eef a863b5bb help.de.txt		TEXT FI		Ling/partition_1/initrd/FILE		https://www.gnu.org/licenses	
191204	893666ec92c37ctrad57a76c187648b	415d32ee5028d8994i Getde4bf315504bb9 Jogname.coreutils		FLF		Umg/partition_1/initrd/FILE		https://translationproject.org/team	
191204	c5368a3e14a75c561t9e141t75bcadb			£1,7		Ling/partition_1/initrd/Fild		https://ext4.wiki.kemei.org/index.php/bigalioc	
191204	16726219ad93803c6f54cf96d6c19c			FLF		Img/partition_1/initrd/FILE		http://www.openssi.org	
291204	003a49b00c4335454d8f2ff0059748b	e3cd48cG19c407Gc58 e12baf82z4e34a350izionste	/sample C3.img/partition.1/initrd/FILE/usr/bin/zipnote	FLF	RegularFil/tarrole CS	Umg/partition_1/initrd/FILE	www.info.zig.org	www.info.zip.org	
391204	c6e1448ae1184ac79a378e134fdd2a7			TEXT FI		Ling/partition_1/initrd/FILE		http://www.xkpd.com/588	
291204	59e0cdea195bf8e9c101d1c81e62078	8a6790505485ba785c560a4a8ac4fb4cd1401psec				Umg/partition_1/initrd/FILE		http://www.fsf.org/copyleft/gol.txt	
191204				EU/		Ime/partition 1/initrd/FiLE		http://www.enu.ore/software/findutils	
291204	bb273c0fea5524a8efea443befbcid96	d569c7fd8476be700r064ba9908dcf70148d gawk-4.2.1	/sample_C3.img/partition_1/initrd/FILE/usr/bin/gawk-4.2.1	ELF	RegularFil/sample_C5	Ume/partition_1/initrd/FILE	WHOM BOILOGE	https://www.enu.org/software/gawk/manual/html_node/Bugs.html	
291204	12972c6ds2c6f63e4df5f3e62d72794	Scaf43b1a fad4e134t bcfd1ebai e34c1cb94 dir.coreutils	/sample_C3.img/partition_1/initrd/FILS/usr/bin/dir.coroutils	ELF.	RegularFil/sample C5	Ling/partition_1/initrd/FiLE	wiki sich ore	https://wki.xiph.org/MIME Types and File Extensions	
391204	p0f38191d063aeb0135ea9bc3cba7cb	af374e78c bs4ct2b212fb790d8f4dd119e4 services	/sample_C3.img/partition_1/initrd/FILE/etc/services	ASCIL		umg/partition_1/initid/FILE		http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services	
291204	7905ddd2e51dbe1ecbed5108ca0idee	AVAILAB F32 efekteds 7: 201426:44 Mbit21c2at dimmar	/vample_CS.img/partition_1/initrd/FILS/uar/bin/dimmar	FLF		ump/pertition 1/mitrd/FILE		http://http-keys.gnupg.net	
291204	7905ddd2e63dbe1ecbe46108ca43dee	799086f52 efe31db7 289426644 6b823c2at dimmer	/semale C5.mg/pertition_1/mitrd/FIL5/psr/bin/dimmer	ELF	RegularFil/sample CS	imp/partition_1/initrd/FILE	versions.enuos.org	https://versions.enupe.org/swdb.bt.sig	
291204	aTte2bc1d800d5e289a7bc897d94106	a139c7665 adoc109d, 1307137bi (a867aba3 grep.grep	/semple_C5.img/partition_1/initrd/FILE/bin/grep.grep	FLF	RegularFil/sample CS	Ling/partition_1/mitrd/FILE	gil sy proces	http://pit.sv.gnu.mp/git/prep.pit/tree/AUTHORS	
			/sample CS.imp/partition_1/initrd/FILE/usr/lib6t/ssl-1.1/ct_log_list.onf.di-	ASCIL		img/partition_1/initrd/FILE		https://pithub.com/poople/certificate-transparency/blob/master/python/uti	lities/log
221201	01fd93debbdd+baste39e28c304026a	d5a93561126/202232i0000a282id5daae811ed5.min.is	/sample_C5.img/partition_1/initrd/FILE/ril/ServerRoot/htdocs/eds.min.is	IAVASC	Ri Regularfil/sample CS	Lime/oartition.1/inited/FILE	www.medbox.com	https://www.mapbox.com/api-documentation/#access-tokens":function	
391204	65fd83debbdd+bballe33+28c3fd424a		/semale_C5.ims/partition_1/initrat/FilE/ril/ServerBoot/htdocs/eds.min.is					https://www.masbux.com/".e.setAttribute("aria-label", "Mapbox	
391204	b1foe6d153664f351949c02405ab0a7	428a22cb15028d3dei 8751be90; d49bd65ti libumi2, so, 2,9,8	/sample_C5.img/partition_1/initrd/FILE/usr/lib64/libornt2.so.2.9.8	ELF	RegularFil/sample CS	Ling/partition_1/initrd/FiLE	www.asoc.net	http://www.ascc.net/sml/schematron	
391204	doe0491151bcace5011e1c817281011	cbc7ed9bc0ace3798C8093275dr613ab09crC07IP_DECOMPRESSED.000043b1	/sample_C5./ms/partition.1/bitmare/62/P_DFCCMPR/55FD.000943b1	FLF	Regularfil/sample C5	Ling/partition.1/brimage	www.kernel.org	https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/litt.html	
391204		0250dt3b128a369751158bt7800 da739ebd gpgcont		ELF		Umg/partition_1/initrd/FiLE		https://gnu.org/licenses	
				ELF.		Ling/partition_1/initrd/FLE		https://bugs.gtupg.org	
391204	Bfeea719d99c3501fbf7e787e741596			ELF		Ling/partition_1/initrd/FILE		http://gnu.org/licenses/gpl.html	
				FLF		Ling/partition_1/initrd/FILE		https://ext4.wiki.kemel.org/index.phg/Rigslioc	
391204				ELF		Lime/partition_1/initrd/FILE		https://ext4.wiki.kemel.org/index.php/8jgalloc	
						img/partition_1/initrd/FILE		https://www.enu.org/licenses/gol.html	
				EUF		Lime/partition_1/initrd/FiLE		ftp://ftp.info.zip.org/pub/infozip	
				FIF		Ling/partition_1/initrd/FILE		http://www.info.zip.org	
		a seal file as servery a bed as sea file of the hilling						in the second se	

ASCII ASCII

2023-08-09121:30:17.391204 050f381510663eb0 < > <u>c5\_url-strings</u> +

Figure 154: C5 Infoleak URL Report (Jarvis)

/58

.

http://www.opensol.org/sosignm http://www.iana.org/assignm http://www.iana.org/assignm

1/mbd/HLE www.iana.org 1/mbd/HLE www.iana.org

# **APPENDIX H: EFFECT OF ALGORITHM CHANGES**

Artifact Risk Summary Published: September 01, 2023

Evaluation Sample 6 / Test

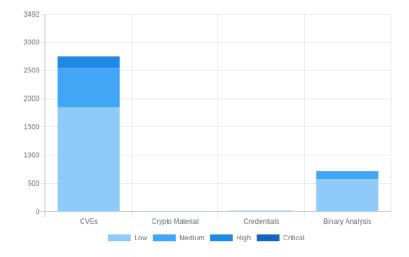
FINITE STATE

**ARTIFACT ANALYSIS** 

# **Artifact Analysis**

Finite State analyzes artifact to detect potential risks and vulnerabilities due to user accounts configuration errors, hard coded or easily guessed credentials, software components and CVEs, hard coded crypto materials, and binary analysis.

3492 Findings by Type Breakdown

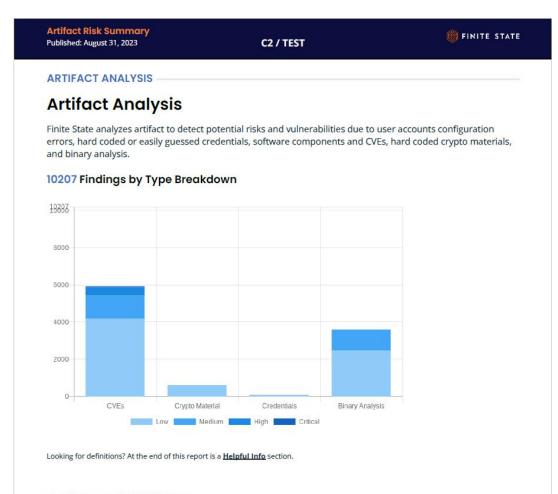


Looking for definitions? At the end of this report is a <u>Helpful Info</u> section.

### Finding Exploit Intelligence

Category	Count
No Known Exploits	2413 Findings
Proof of Concept Exploit	1038 Findings
Weaponized	41 Findings
Reported in the Wild	11 Findings
Exploited by Threat Actors	6 Findings

Figure 155: Scan of C2 Prior to Algorithm Changes.



### **Finding Exploit Intelligence**

Category	Count	
No Known Exploits	8288 Findings	
Proof of Concept Exploit	1833 Findings	
Weaponized	86 Findings	
Reported in the Wild	27 Findings	
Exploited by Threat Actors	17 Findings	

Figure 156: Scan of C2 Following Algorithm Changes.