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

DAKOTA STATE UNIVERSITY

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: 7483337

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

Graduate Office Verification: DocuSigned by: Abby Chowning F44C8D9E621C417... Date: 11/06/2023

Dissertation Chair/Co-Chair: DocuSigned by: Kyle Cronin 9B9AFA1BE48843C... Date: 11/06/2023
Print Name: Kyle Cronin

Dissertation Chair/Co-Chair: _____ Date: _____
Print Name: _____

Committee Member: DocuSigned by: Dr. Bassam Farroha 859126720BE14A7... Date: 11/06/2023
Print Name: Dr. Bassam Farroha

Committee Member: DocuSigned by: Dr. Michael Ham 7499B29D70C7542A... Date: 11/06/2023
Print Name: Dr. Michael Ham

Committee Member: DocuSigned by: Dr. Viki Johnson 400E68A5C00E40E... Date: 11/06/2023
Print Name: Dr. Viki Johnson

Committee Member: DocuSigned by: Dr. Gale Pomper 4B4F6F22DC5A41F... Date: 11/06/2023
Print Name: Dr. Gale Pomper

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 quasi-experiment 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. Begian__

Charles H. Begian

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

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).

Table 1: Classes of 5G Wireless Access Points

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)

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 quasi-experiment 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 "α") and a Type II (false negative) error rate of 10% denoted as "β"). Creswell suggests "commonly accepted" α and β values of 0.05 and 0.20, respectively (Creswell & Creswell, 2017), but this study attempted to achieve a lower β value (0.10) and a statistical power >= 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 β 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 (ϵ) is small but not zero ($0 < \epsilon < \left(\frac{1}{T}\right)$) and decreases as *T* increases.

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

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 sub-question. 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) 5G 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 → 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 variabl*e: 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 β 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 Chinese-produced (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: Commercial 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).

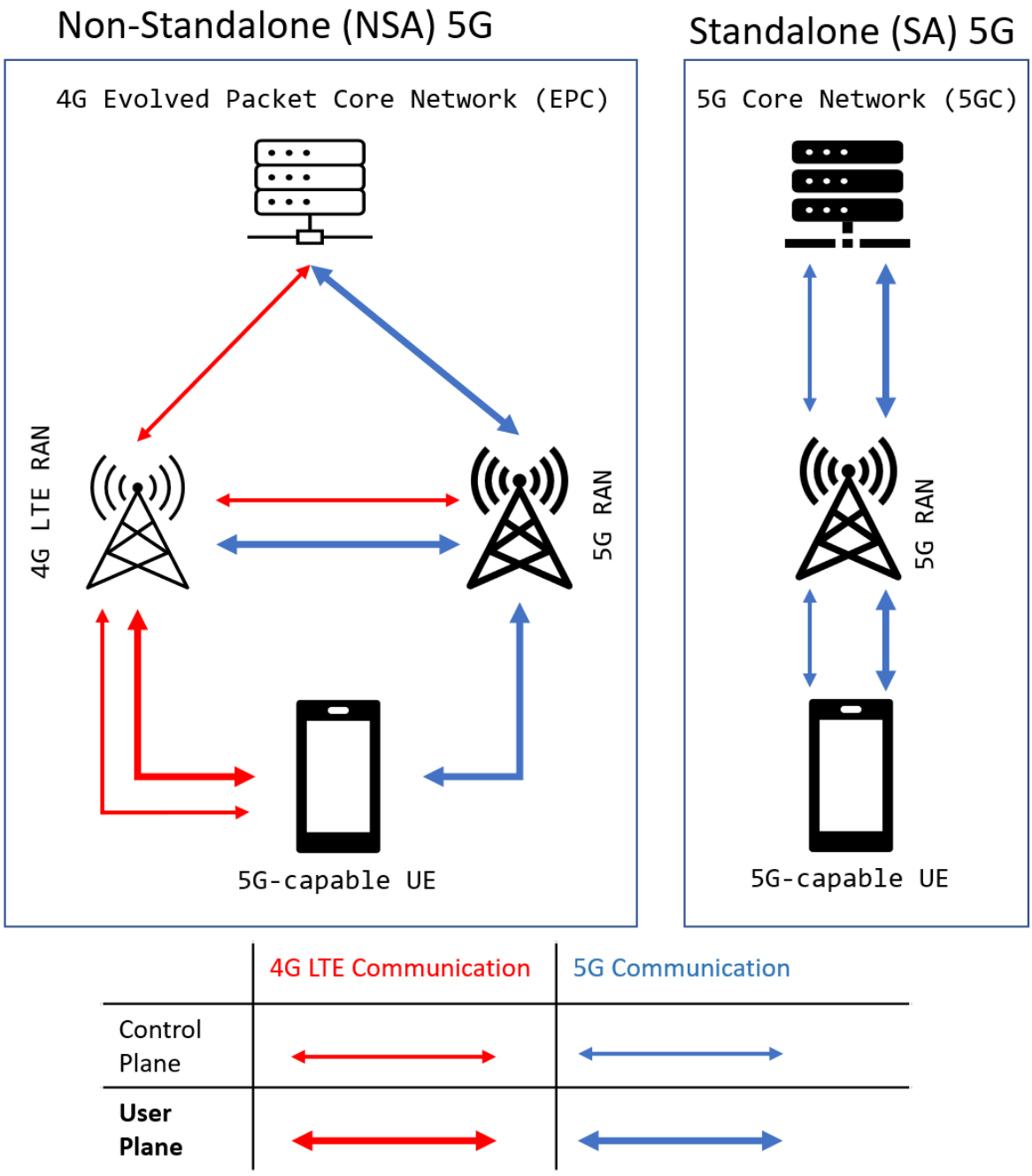


Figure 1: Non-standalone and Standalone 5G

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. 5G network device manufacturers may be inclined to serve the larger, 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 116th 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).

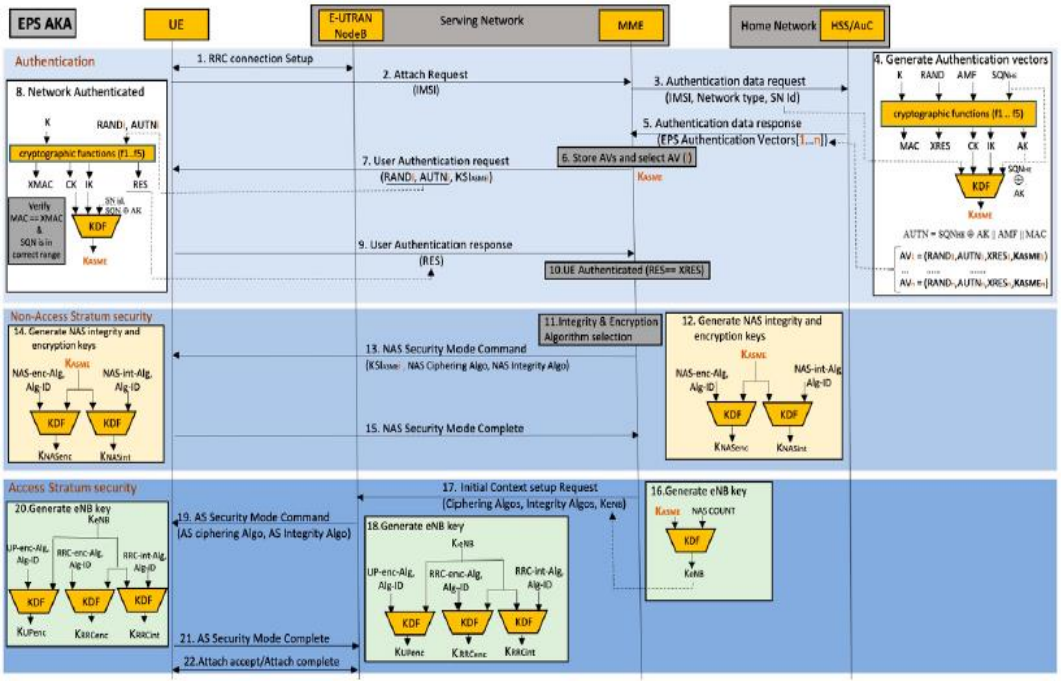


Figure 2: 4G LTE Authentication (Dhanasekaran, 2023)

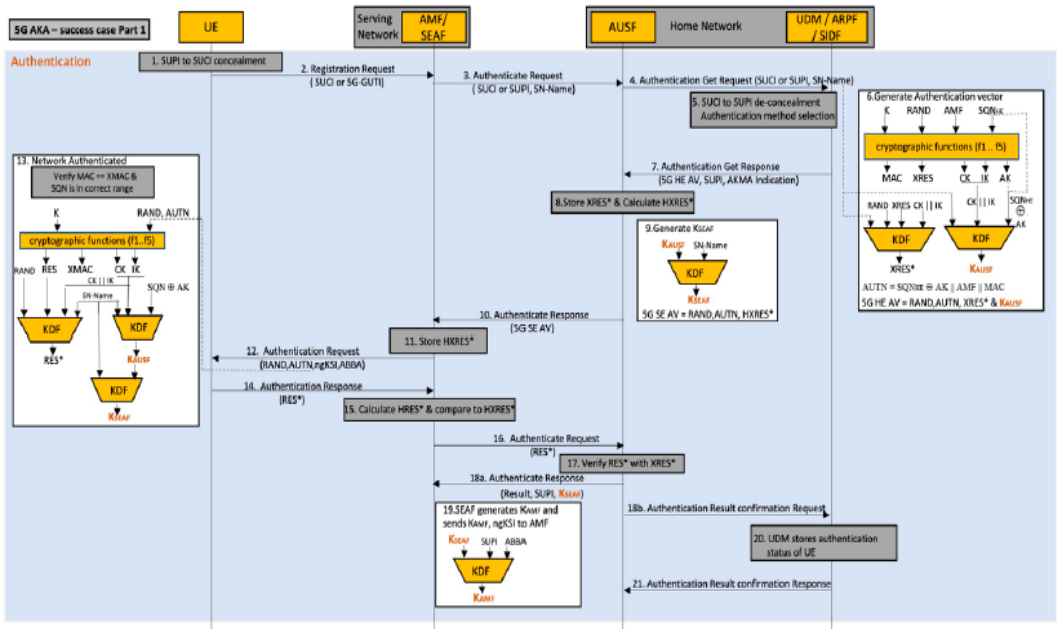


Figure 3: 5G Authentication (Dhanasekaran, 2023)

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.

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

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

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

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 {
    j = 0
    MFG = A_i
    WHILE ( P.size() < N ) AND ( j < MFG.size() ) DO {
        P.append( MFG_j )
        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, ϵ, 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	TOOL VERSION	SAMPLE ELEMENT	FIRMWARE VERSION	RUN DATE/TIME START	RUN DATE/TIME END	PLATFORM	OS VERSION	VULN 1	C1	VULN 2	C2	VULN 3	C3
TOOL-01	1.5	Nokia01	3.88	5/22/22 9:56 AM	5/23/22 10:10 AM	64-bit PC, 32GB RAM	Linux 20.0	CVE-2021-mmmmm	0.8	CVE-2018-nnnnn	0.4	CVE-2022-zzzzz	1
TOOL-01	1.5	Nokia02	2.72	5/26/22 7:00 AM	5/26/22 8:18 AM	64-bit PC, 32GB RAM	Linux 20.0	CVE-2021-mmmmm	0.9	CVE-2022-xxxxx	0.1		
TOOL-02	2.0	Huawei01	3.88	5/24/22 1:21 PM	5/25/22 5:28 PM	64-bit PC, 32GB RAM	Linux 20.0	CVE-2021-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 no reported vulnerabilities are still to be considered free of vulnerabilities with a confidence

rating of ϵ. 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.

Table 5: 5G Femtocell Purchase Attempts

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 Communications	Only sells to MNOs.
Askey Computer Corp.	Emails to vendor unanswered. Calls to the 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 Systems	Only sells to MNOs
Nokia	Only sells to MNOs
SerComm	Would not sell to a researcher.
Sterlite Technologies	Would not sell just one unit.

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 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." (Tannahill, 2023)*

The 5G firmware analyzed in this study was extracted from used BBU components obtained from Alibaba.com (https://www.alibaba.com) and from a professional contact, Mr. Earl Lum (https://www.ejlwireless.com). 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.

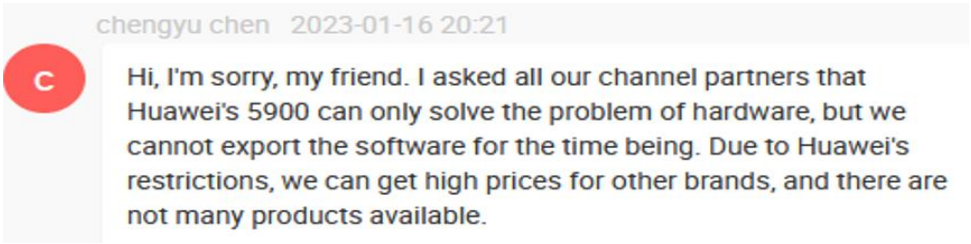


Figure 5: Huawei restricts export of software.

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.

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

Manufacturer	Model	Type
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

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.

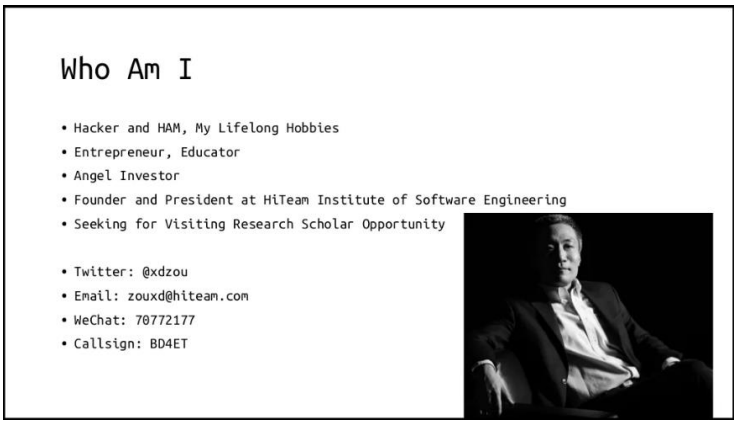


Figure 8: Xiaodong Zou

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.

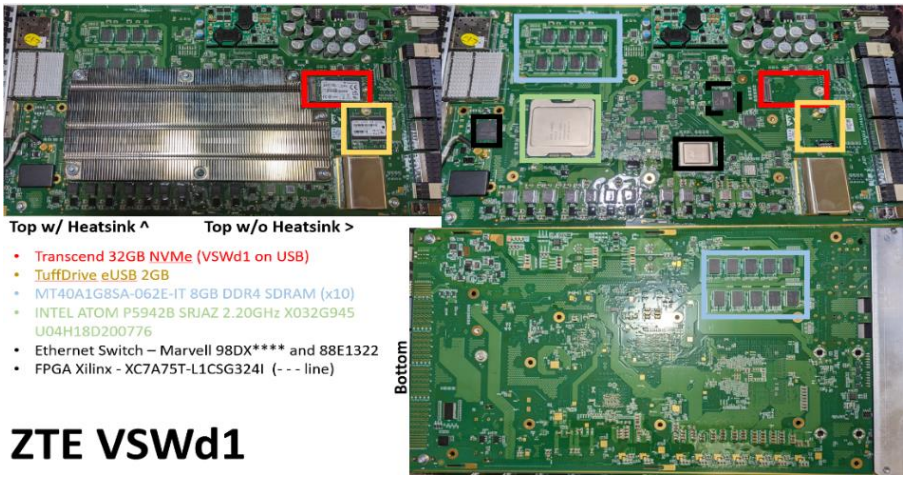


Figure 9: ZTE VSWd1 controller board.

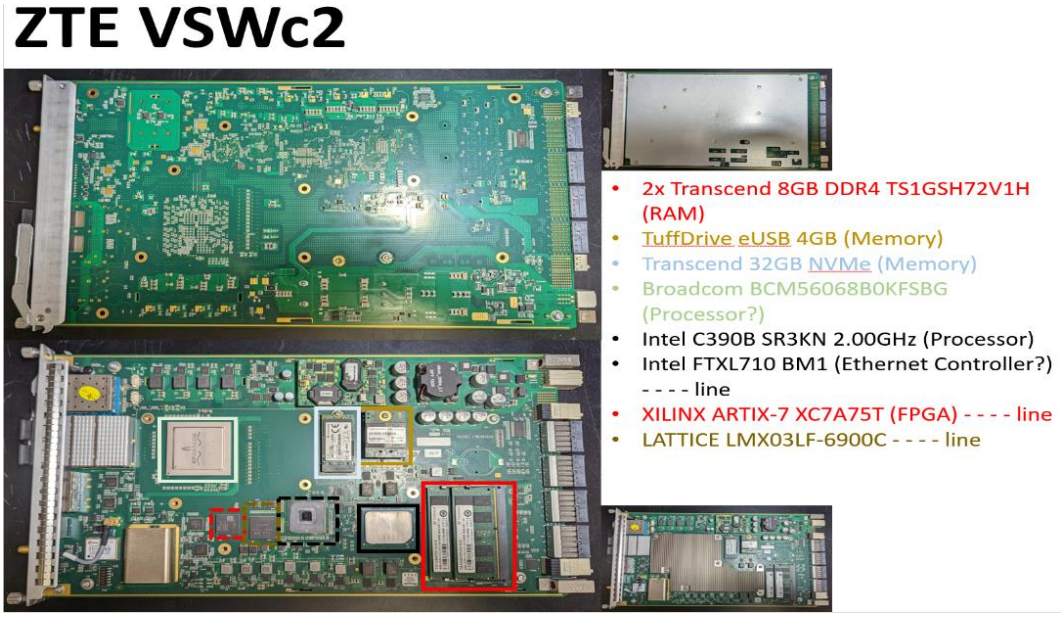


Figure 10: ZTE VSWc2 controller board

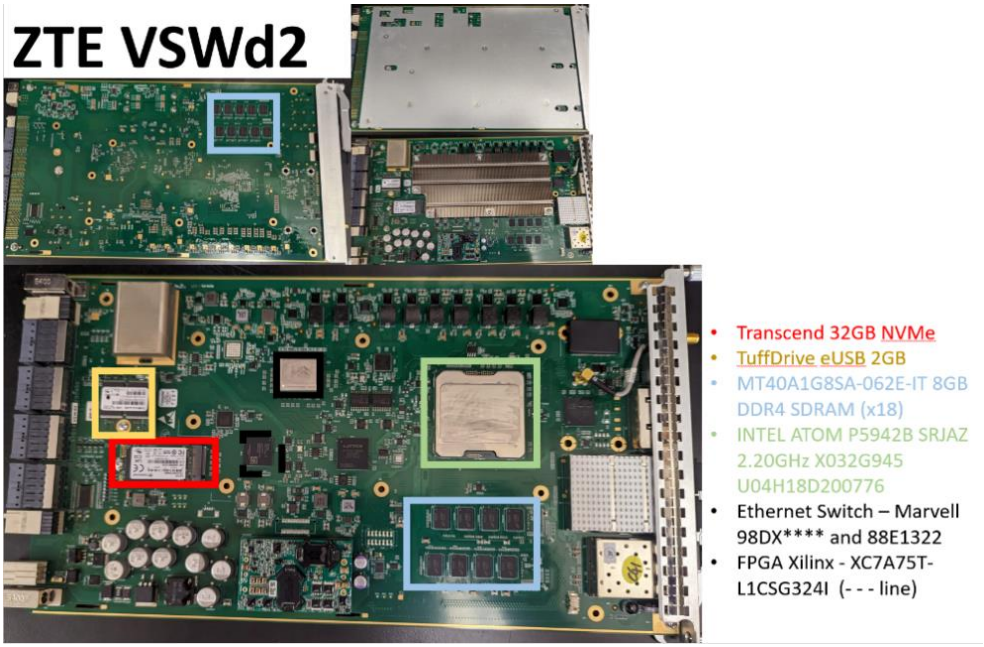


Figure 11: ZTE VSWd2 controller board

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.

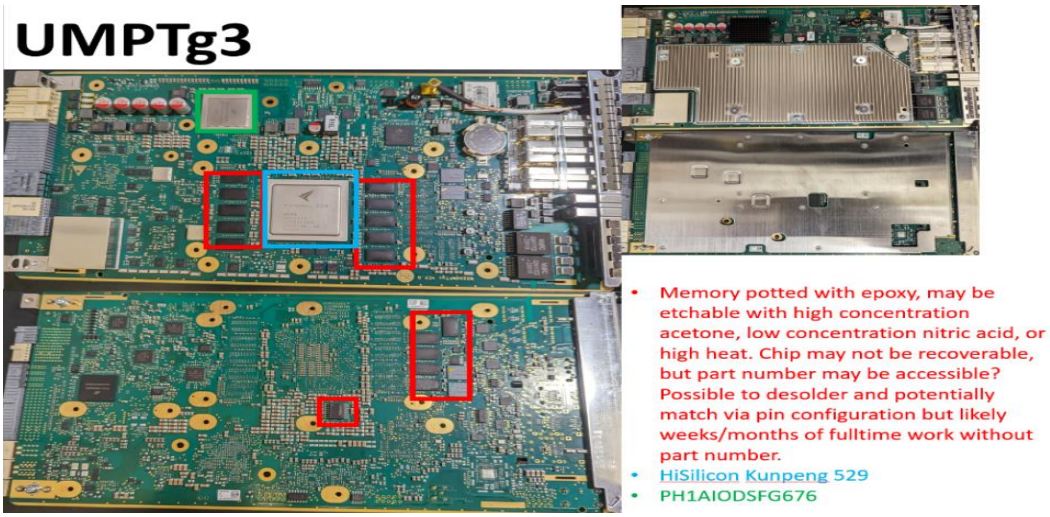


Figure 12: Huawei UMPTg3 with epoxied memory modules

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.

Table 7: Firmware samples, sizes, and identifiers.

Sample Identifier	Firmware	Size	Zipped (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

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 M_1-M_4 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.

Table 8: Number of Unique CVEs Identified in each Sample

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

Table 9: CVE findings C values

#CVEs with *C*:	C1	C2	C3	C4	C5
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

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.

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

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

Table 11: 454 Common CVEs by Group

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		

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_0 and H_1

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 ϵ (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.

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

Sample	Number of CVEs Reported by Multiple CSTs ($C > 0.25$)	Number of CVEs Reported by a Single CST ($C = 0.25$)	Ratio of CVEs Reported (Multiple 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

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 $C >= 0.75$). 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.

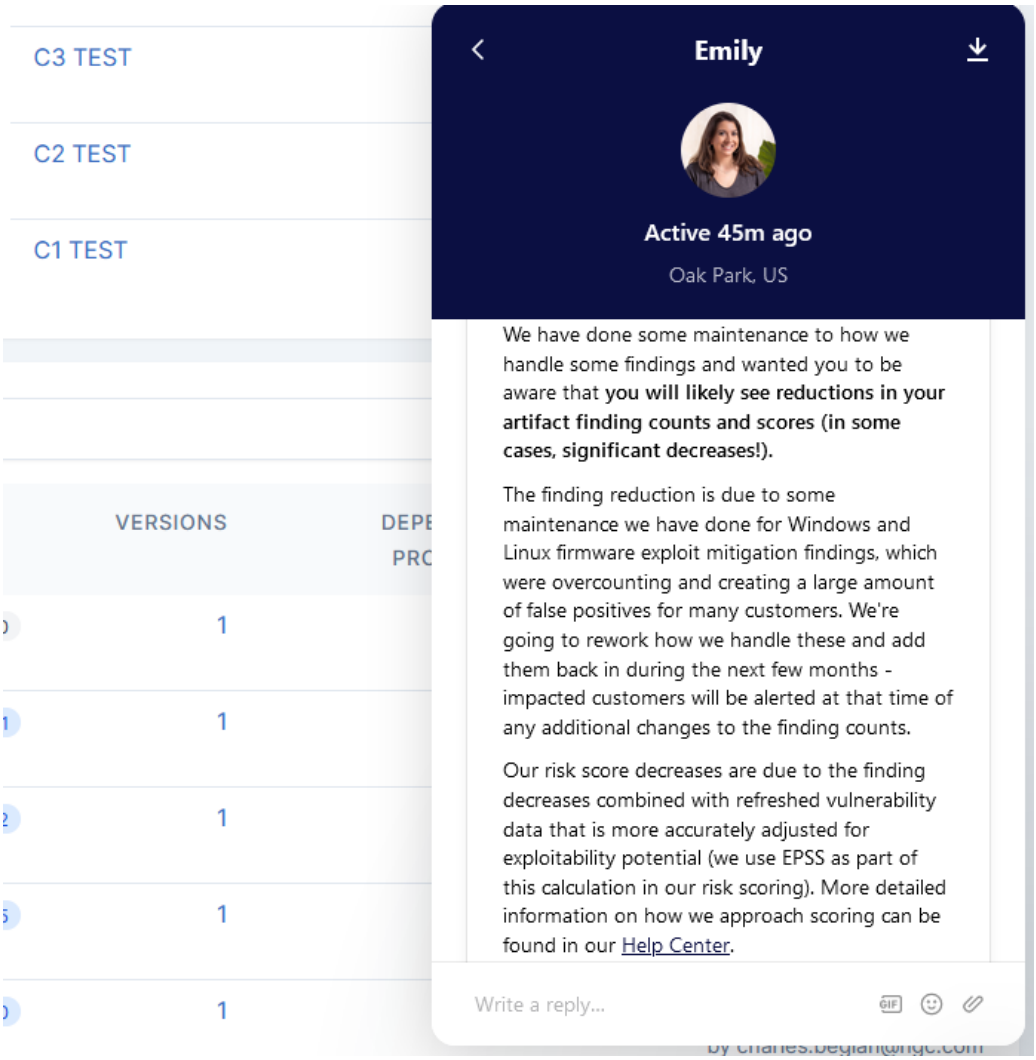


Figure 13: Finite State Algorithm Changed to Reduce False Positives.

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_1: 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_2: 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_3: 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 M_4: 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.

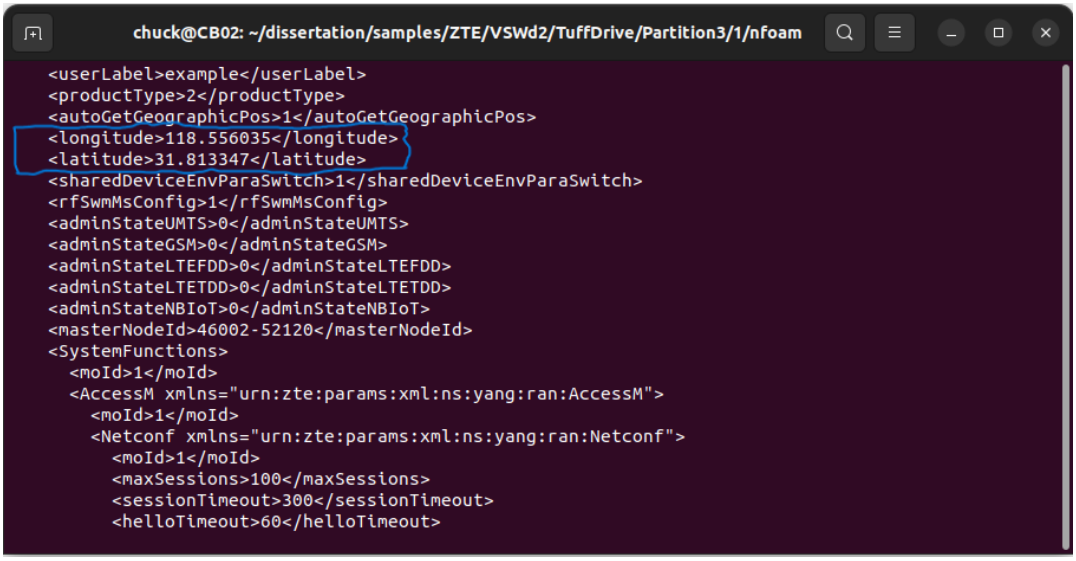


Figure 14: Geocoordinates of ZTE VSWd2 BBU.

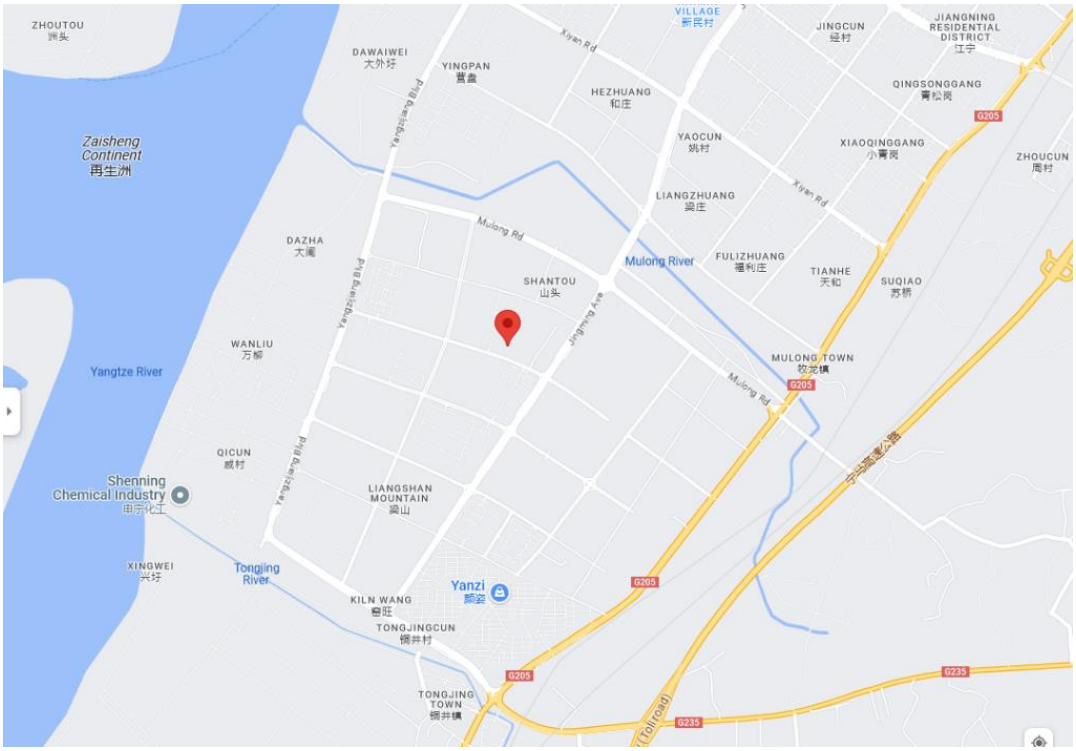


Figure 15: Corresponding Location of ZTE VSWd2 BBU, SW of Nanjing, China.

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_1-M_4

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 (ϵ) 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 https://about.att.com/story/2019/tyndall_air_force_base.html

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.qnx.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 https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/ultra-services-platform/5g-ran-indoor.pdf

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 https://onestore.nokia.com/asset/210846

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 https://www.defense.gov/Newsroom/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati/
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 https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/indoor-outdoor
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 https://www.federalregister.gov/d/2022-28263
Finite State. (2019a). *Finite State Supply Chain Assessment*. Retrieved from
Finite State. (2019b). Finite State Responds to Huawei. Retrieved from https://finitestate.io/blog/finite-state-responds-to-Huawei-Critiques-stands-by-assessment-huawei-products-contain-significant-vulnerabilities
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 https://finitestate.io/products/finite-state-platform/
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 https://www.grammatech.com/our-products/codesentry/

GSMA Intelligence. (2020). *Mobile Economy 2020 North America*. Retrieved from Los Angeles: https://www.gsma.com/mobileeconomy/northamerica/

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 https://www.huawei.com/en/psirt/security-notices/huawei-sn-20190702-01-finitestate-en

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 https://www.jstor.org/stable/26994111

Lum, E. (2023). RF SMP Board-to-Board Connectors Market Review. *Microwave Journal, 66*(3), 86-88,90,92. Retrieved from https://www.microwavejournal.com/articles/39786-rf-smp-board-to-board-connectors-market-review

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 https://www.cve.org/

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 https://www.jstor.org/stable/24430332

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 https://www.nccoe.nist.gov/5g-cybersecurity

NIST. (2023). National Vulnerability Database. Retrieved from https://nvd.nist.gov/general/nvd-dashboard

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 https://digitallibrary.sdsu.edu/islandora/object/sdsu%3A59794 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 https://www.ft.com/content/2534ca85-b08e-4f78-88f3-c04770b41a02

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 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

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 https://www.synopsys.com/software-integrity/security-testing/software-composition-analysis/binary-analysis.html

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 https://www.hsdl.org/?view&did=458706

Verizon. (2020). What are phone bands (GSM, CDMA) and why do they matter? Retrieved from https://www.verizon.com/articles/Smartphones/what-are-phone-bands-and-why-do-they-matter/

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 (*).

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

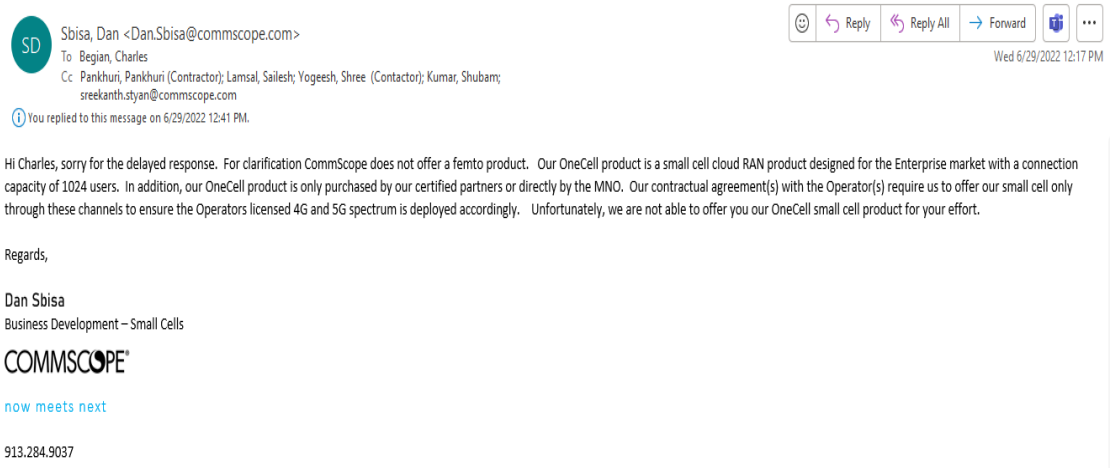
CVE-2009-5155	CVE-2019-18805	CVE-2020-27066	CVE-2021-38604	CVE-2022-26490
CVE-2013-0340	CVE-2019-19126	CVE-2020-27068	CVE-2021-3864	CVE-2022-27666
CVE-2013-4235	CVE-2019-19252	CVE-2020-27618	CVE-2021-39537	CVE-2022-27774
CVE-2014-2524	CVE-2019-19319	CVE-2020-27675	CVE-2021-39633	CVE-2022-27776
CVE-2015-0569	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

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.



SD Sbisa, Dan <Dan.Sbisa@commscope.com>
To Begian, Charles
Cc Pankhuri, Pankhuri (Contractor); Lamsal, Sailesh; Yogeesh, Shree (Contactor); Kumar, Shubam; sreekanth.styan@commscope.com
You replied to this message on 6/29/2022 12:41 PM.

Reply | Reply All | Forward
Wed 6/29/2022 12:17 PM

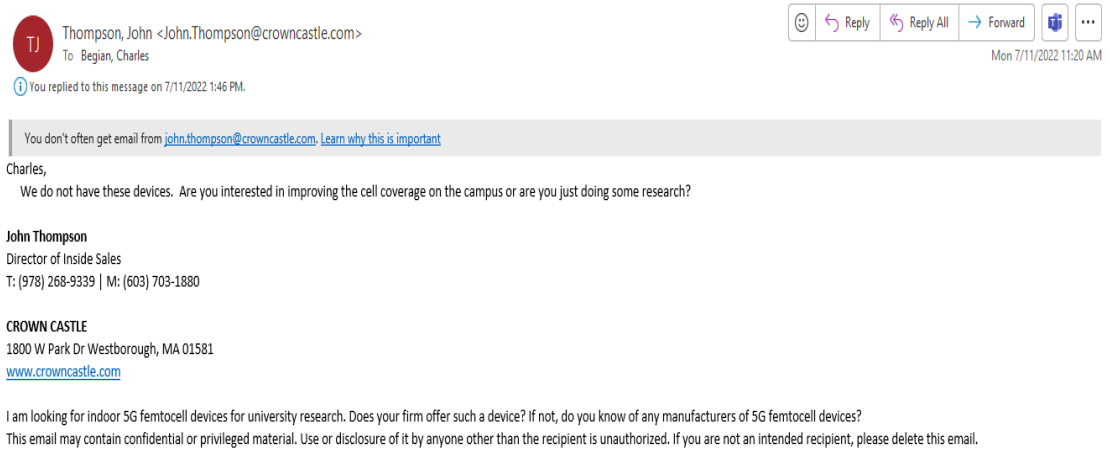
Hi Charles, sorry for the delayed response. For clarification CommScope does not offer a femto product. Our OneCell product is a small cell cloud RAN product designed for the Enterprise market with a connection capacity of 1024 users. In addition, our OneCell product is only purchased by our certified 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.

Regards,

Dan Sbisa
Business Development – Small Cells
COMMSCOPE
now meets next

913.284.9037

Figure 16: CommScope Response (Sbisa, 2022)



TJ Thompson, John <John.Thompson@crowncastle.com>
To Begian, Charles
You replied to this message on 7/11/2022 1:46 PM.

Reply | Reply All | Forward
Mon 7/11/2022 11:20 AM

You don't often get email from john.thompson@crowncastle.com. Learn why this is important

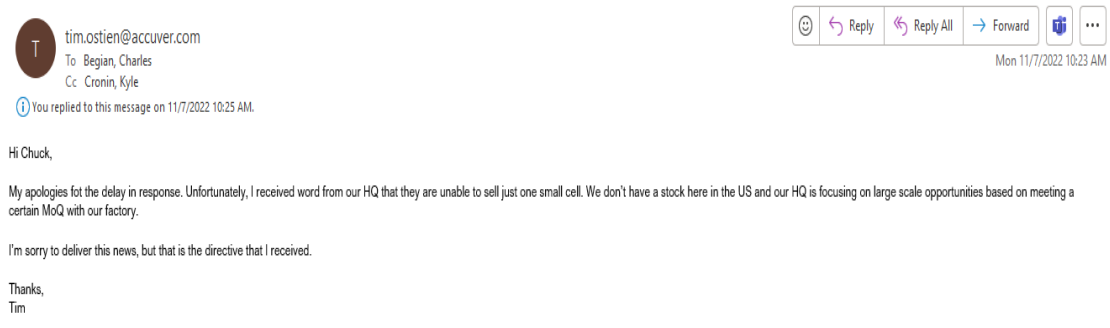
Charles,
We do not have these devices. Are you interested in improving the cell coverage on the campus or are you just doing some research?

John Thompson
Director of Inside Sales
T: (978) 268-9339 | M: (603) 703-1880

CROWN CASTLE
1800 W Park Dr Westborough, MA 01581
www.crowncastle.com

I am looking for indoor 5G femtocell devices for university research. Does your firm offer such a device? If not, do you know of any manufacturers of 5G femtocell devices?
This email may contain confidential or privileged material. Use or disclosure of it by anyone other than the recipient is unauthorized. If you are not an intended recipient, please delete this email.

Figure 17: Crown Castle Response (Thompson, 2022)



T tim.ostien@accuver.com
To Begian, Charles
Cc Cronin, Kyle
You replied to this message on 11/7/2022 10:25 AM.

Reply | Reply All | Forward
Mon 11/7/2022 10:23 AM

Hi Chuck,

My apologies fot 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.

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

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

Reply | Reply All | Forward

Fri 1/27/2023 11:40 AM

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: www.fcc.gov/kdb 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

C colin@hbscheng.com
To Begian, Charles

Reply | Reply All | Forward

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.
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: Begian, Charles
Date: 2023-01-31 00:16
To: colin@hbscheng.com
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 <Charles.Begian@trojans.dsu.edu>
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

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

APPENDIX C: CST SCAN REPORT EXCERPTS FOR SAMPLE C1

Sample C1 Black Duck Scan Report Excerpts

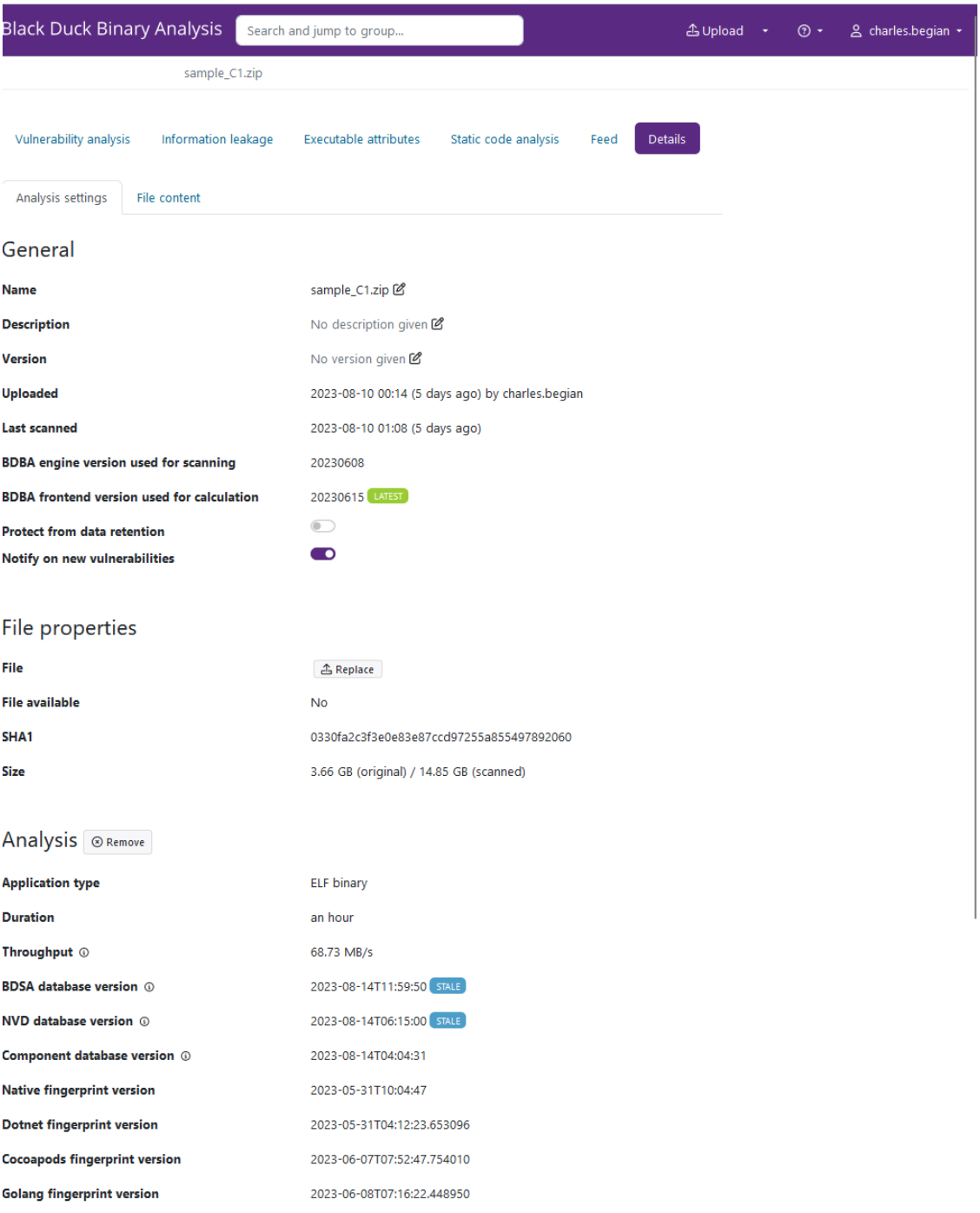


Figure 22: C1 Scan Overview (Black Duck)

Report generated 2023-08-13T22:21:06Z
https://protecode-sc.com/products/24698186

sample_C1.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY

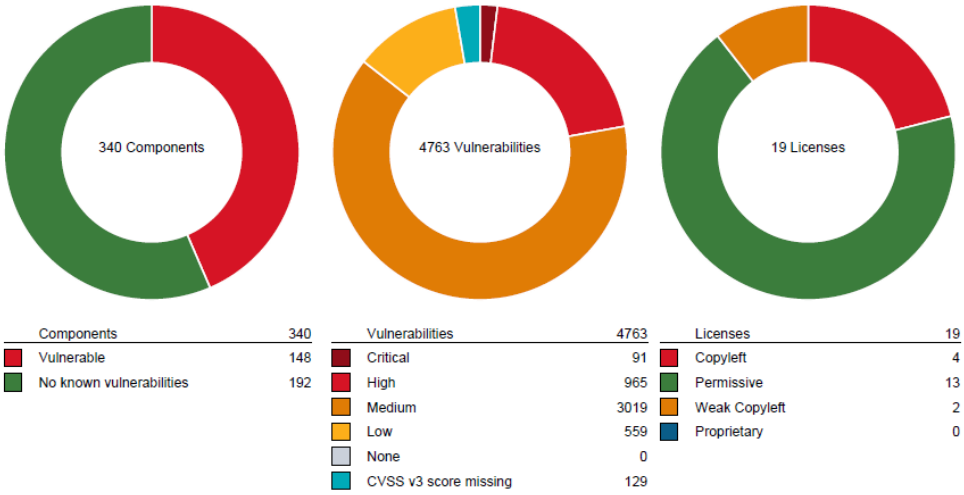


Figure 23: C1 Scan found 4763 Vulnerabilities (Black Duck)

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

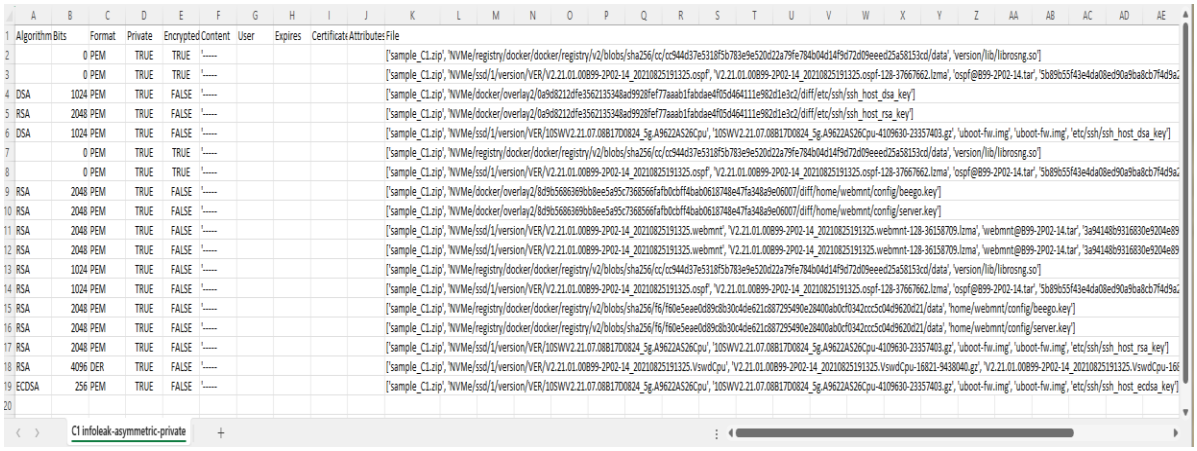
Details

Original filename	
SHA1 checksum	0330fa2c3f3e0e83e87ccd97255a855497892060
Original file size	3661.65 MB

Infoleak

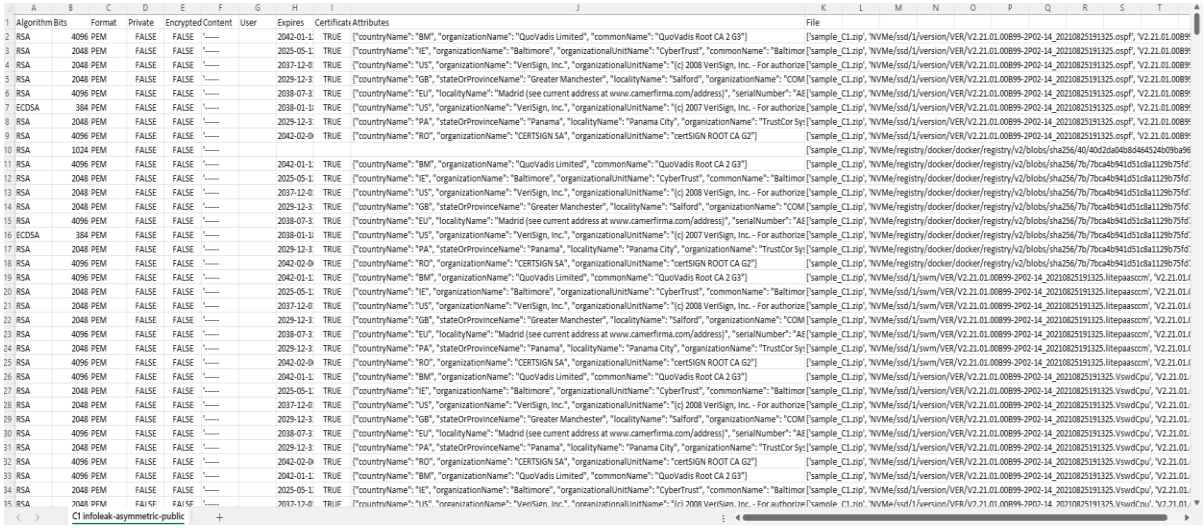
Asymmetric keys:	725
AWS keys:	0
Custom pattern matches:	0
Emails:	12945
HTTP authentication:	0
Image metadata:	0
IP addresses:	9597
JSON web tokens:	0
MAC addresses:	152
OAuth tokens:	0
Passwords:	387
Shell history:	6
URLs:	6555
Twilio keys:	0
Google cloud keys:	0
Facebook access tokens:	0

Figure 24: C1 Information leaks (Black Duck)



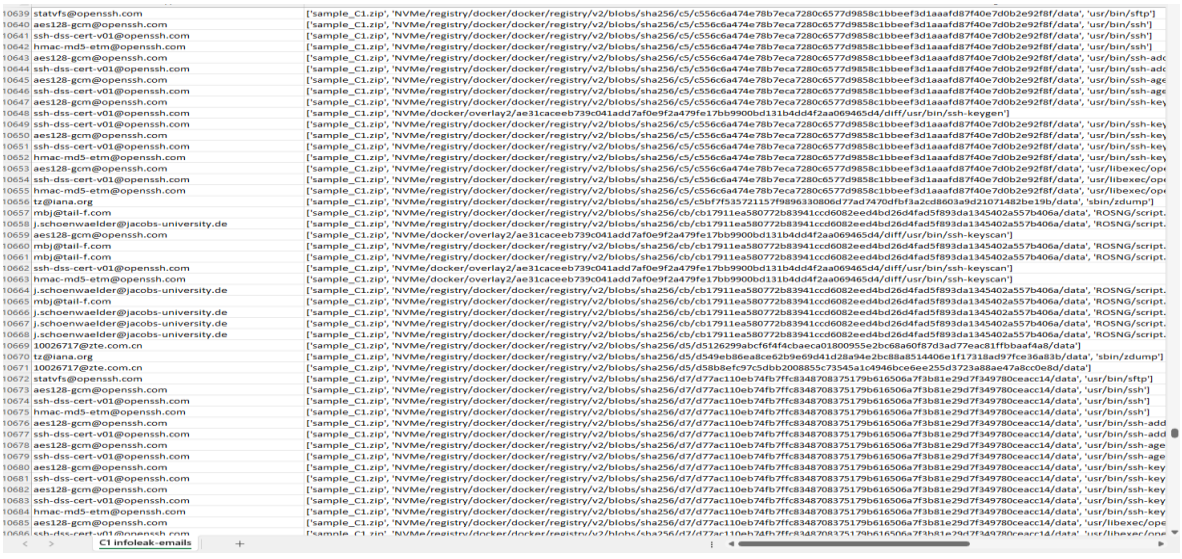
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE
1	Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File																				
2		0	PEM	TRUE	TRUE	'-----					['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cc/cc944d37e5318f5b783e9e520d22a79fe784b04d14f9d72d09eeed25a58153cd/data', 'version/lib/librosng.so']																				
3		0	PEM	TRUE	TRUE	'-----					['sample_C1.zip', 'NVMe/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', '5b89b55f43e4da08ed90a9ba8cb7f4d9a2																				
4	DSA	1024	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/etc/ssh/ssh_host_dsa_key']																				
5	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/etc/ssh/ssh_host_rsa_key']																				
6	DSA	1024	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g.A9622A526Cpu', '10SWV2.21.07.08B17D0824_5g.A9622A526Cpu-41090630-23357403.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/ssh/ssh_host_dsa_key']																				
7		0	PEM	TRUE	TRUE	'-----					['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cc/cc944d37e5318f5b783e9e520d22a79fe784b04d14f9d72d09eeed25a58153cd/data', 'version/lib/librosng.so']																				
8		0	PEM	TRUE	TRUE	'-----					['sample_C1.zip', 'NVMe/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', '5b89b55f43e4da08ed90a9ba8cb7f4d9a2																				
9	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/docker/overlay2/8d9b5686369bb8ee5a95c7368566fafb0cbff4bab0618748e47fa348a9e06007/diff/home/webmnt/config/beego.key']																				
10	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/docker/overlay2/8d9b5686369bb8ee5a95c7368566fafb0cbff4bab0618748e47fa348a9e06007/diff/home/webmnt/config/server.key']																				
11	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/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', '3a94148b9316830e9204e89																				
12	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/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', '3a94148b9316830e9204e89																				
13	RSA	1024	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cc/cc944d37e5318f5b783e9e520d22a79fe784b04d14f9d72d09eeed25a58153cd/data', 'version/lib/librosng.so']																				
14	RSA	1024	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/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', '5b89b55f43e4da08ed90a9ba8cb7f4d9a2																				
15	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/f6/f60e5eae0d89c8b30c4de621c88795490e28400ab0cf0342ccc5c04d9620d21/data', 'home/webmnt/config/beego.key']																				
16	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/f6/f60e5eae0d89c8b30c4de621c88795490e28400ab0cf0342ccc5c04d9620d21/data', 'home/webmnt/config/server.key']																				
17	RSA	2048	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g.A9622A526Cpu', '10SWV2.21.07.08B17D0824_5g.A9622A526Cpu-41090630-23357403.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/ssh/ssh_host_rsa_key']																				
18	RSA	4096	DER	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/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-16																				
19	ECDSA	256	PEM	TRUE	FALSE	'-----					['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g.A9622A526Cpu', '10SWV2.21.07.08B17D0824_5g.A9622A526Cpu-41090630-23357403.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/ssh/ssh_host_ecdsa_key']																				
20																															

Figure 25: C1 Asymmetric keys (Black Duck)



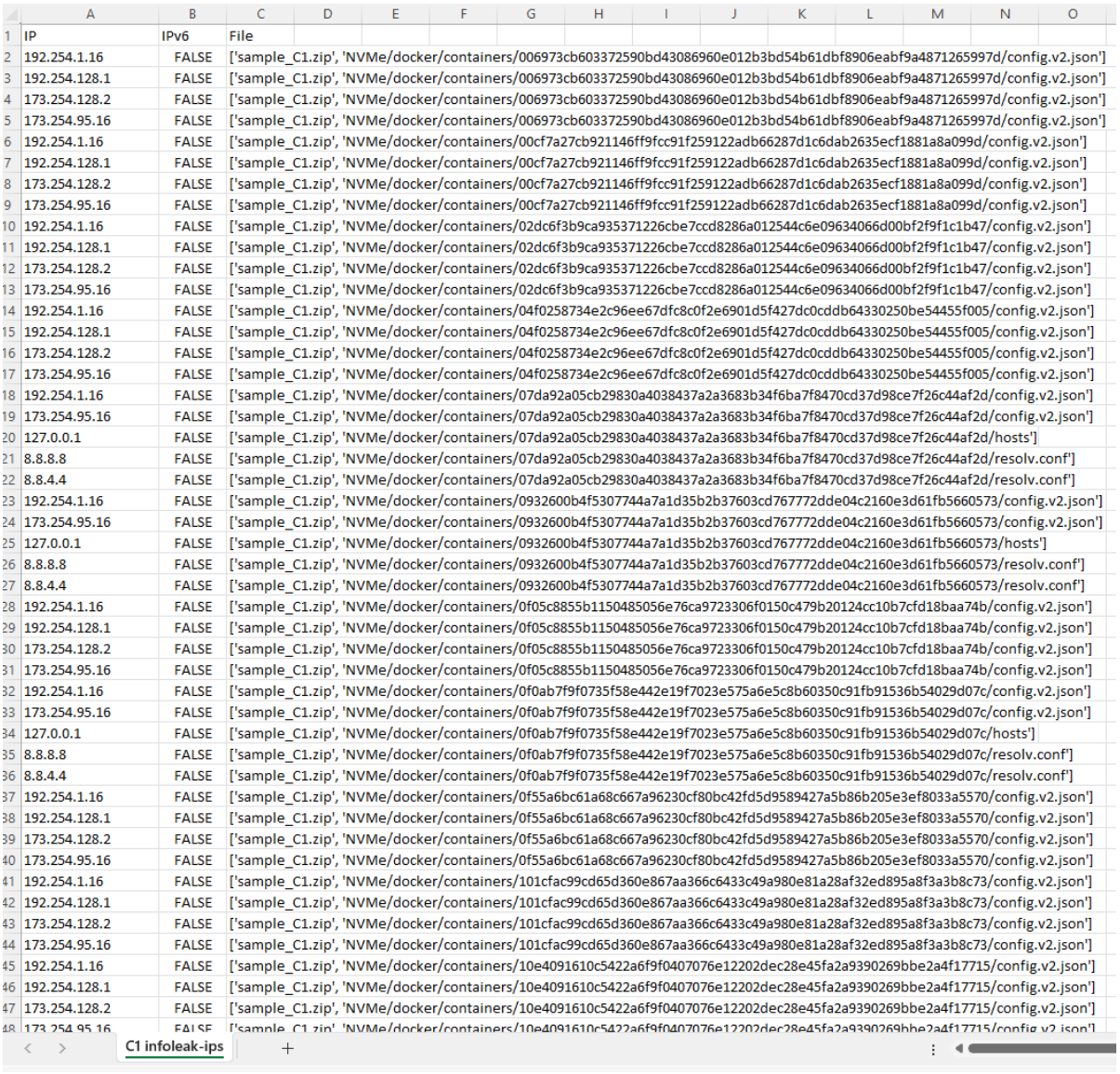
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File									
2	RSA	4096	PEM	FALSE	FALSE	'-----		2042-01-1	TRUE	{"countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 G3"}	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
3	RSA	2048	PEM	FALSE	FALSE	'-----		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.ospf', 'V2.21.01.00899									
4	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/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
5	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COM	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
6	RSA	4096	PEM	FALSE	FALSE	'-----		2038-07-3	TRUE	{"countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "A8	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
7	ECDSA	384	PEM	FALSE	FALSE	'-----		2038-01-1	TRUE	{"countryName": "US", "organizationName": "VeriSign, Inc.", "organizationalUnitName": "(c) 2007 VeriSign, Inc. - For authorize	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
8	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sys	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
9	RSA	4096	PEM	FALSE	FALSE	'-----		2042-02-0	TRUE	{"countryName": "RO", "organizationName": "CERTSIGN SA", "organizationalUnitName": "certSIGN ROOT CA G2"}	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.ospf', 'V2.21.01.00899									
10	RSA	1024	PEM	FALSE	FALSE	'-----					['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/40/40d2da04b8d4645424b09ba96									
11	RSA	4096	PEM	FALSE	FALSE	'-----		2042-01-1	TRUE	{"countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 G3"}	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd									
12	RSA	2048	PEM	FALSE	FALSE	'-----		2025-05-1	TRUE	{"countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimor	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd									
13	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/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd									
14	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COM	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd									
15	RSA	4096	PEM	FALSE	FALSE	'-----		2038-07-3	TRUE	{"countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "A8	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd									
16	ECDSA	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/7bca4b941d51c8a1129b75fd									
17	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sys	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd									
18	RSA	4096	PEM	FALSE	FALSE	'-----		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/7bca4b941d51c8a1129b75fd									
19	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.litepasccm', 'V2.21.01.0									
20	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.litepasccm', 'V2.21.01.0									
21	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.litepasccm', 'V2.21.01.0									
22	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.litepasccm', 'V2.21.01.0									
23	RSA	4096	PEM	FALSE	FALSE	'-----		2038-07-3	TRUE	{"countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "A8	['sample_C1.zip', 'NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepasccm', 'V2.21.01.0									
24	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sys	['sample_C1.zip', 'NVMe/ssd/1/swm/VER/V2.21.01.00899-2P02-14_20210825191325.litepasccm', 'V2.21.01.0									
25	RSA	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.litepasccm', 'V2.21.01.0									
26	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/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
27	RSA	2048	PEM	FALSE	FALSE	'-----		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', 'V2.21.01.									
28	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/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
29	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COM	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
30	RSA	4096	PEM	FALSE	FALSE	'-----		2038-07-3	TRUE	{"countryName": "EU", "localityName": "Madrid (see current address at www.camerfirma.com/address)", "serialNumber": "A8	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
31	RSA	2048	PEM	FALSE	FALSE	'-----		2029-12-3	TRUE	{"countryName": "PA", "stateOrProvinceName": "Panama", "localityName": "Panama City", "organizationName": "TrustCor Sys	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
32	RSA	4096	PEM	FALSE	FALSE	'-----		2042-02-0	TRUE	{"countryName": "RO", "organizationName": "CERTSIGN SA", "organizationalUnitName": "certSIGN ROOT CA G2"}	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
33	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/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									
34	RSA	2048	PEM	FALSE	FALSE	'-----		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', 'V2.21.01.									
35	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/version/VER/V2.21.01.00899-2P02-14_20210825191325.VSwdCpu', 'V2.21.01.									

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-ad
10644	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/bin/ssh-ad
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/op
10654	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/libexec/op
10655	hmac-md5-etm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c556c6a474e78b7eca7280c6577d9858c1bbeef3d1aaafd87f40e7d0b2e92f8f/data', 'usr/libexec/op
10656	tz@iana.org	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/c5/c5bf7f535721157f98963308086d77ad7470dfbf3a2cd8603a9d21071482be19b/data', 'sbin/zdump']
10657	mbj@tail-f.com	['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/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10659	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/docker/overlay2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa069465d4/diff/usr/bin/ssh-keyscan']
10660	mbj@tail-f.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10661	mbj@tail-f.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10662	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/docker/overlay2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa069465d4/diff/usr/bin/ssh-keyscan']
10663	hmac-md5-etm@openssh.com	['sample_C1.zip', 'NVMe/docker/overlay2/ae31caceeb739c041add7af0e9f2a479fe17bb9900bd131b4dd4f2aa069465d4/diff/usr/bin/ssh-keyscan']
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	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/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	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.
10668	j.schoenwaelder@jacobs-university.de	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/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_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d5/d549eb86ea8ce62b9e69d41d28a94e2bc88a8514406e1f17318ad97fce36a83b/data', 'sbin/zdump']
10671	10026717@zte.com.cn	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d5/d58b8efc97c5dbb2008855c73545a1c4946bce6ee255d3723a88ae47a8cc0e8d/data']
10672	statvfs@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/sftp']
10673	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh']
10674	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh']
10675	hmac-md5-etm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh']
10676	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-add
10677	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-add
10678	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-age
10679	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-age
10680	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-key
10681	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-key
10682	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-key
10683	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-key
10684	hmac-md5-etm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/bin/ssh-key
10685	aes128-gcm@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/libexec/ope
10686	ssh-dss-cert-v01@openssh.com	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/d7/d77ac110eb74fb7ffc83487083751796165O6a7f3b81e29d7f349780ceacc14/data', 'usr/libexec/ope

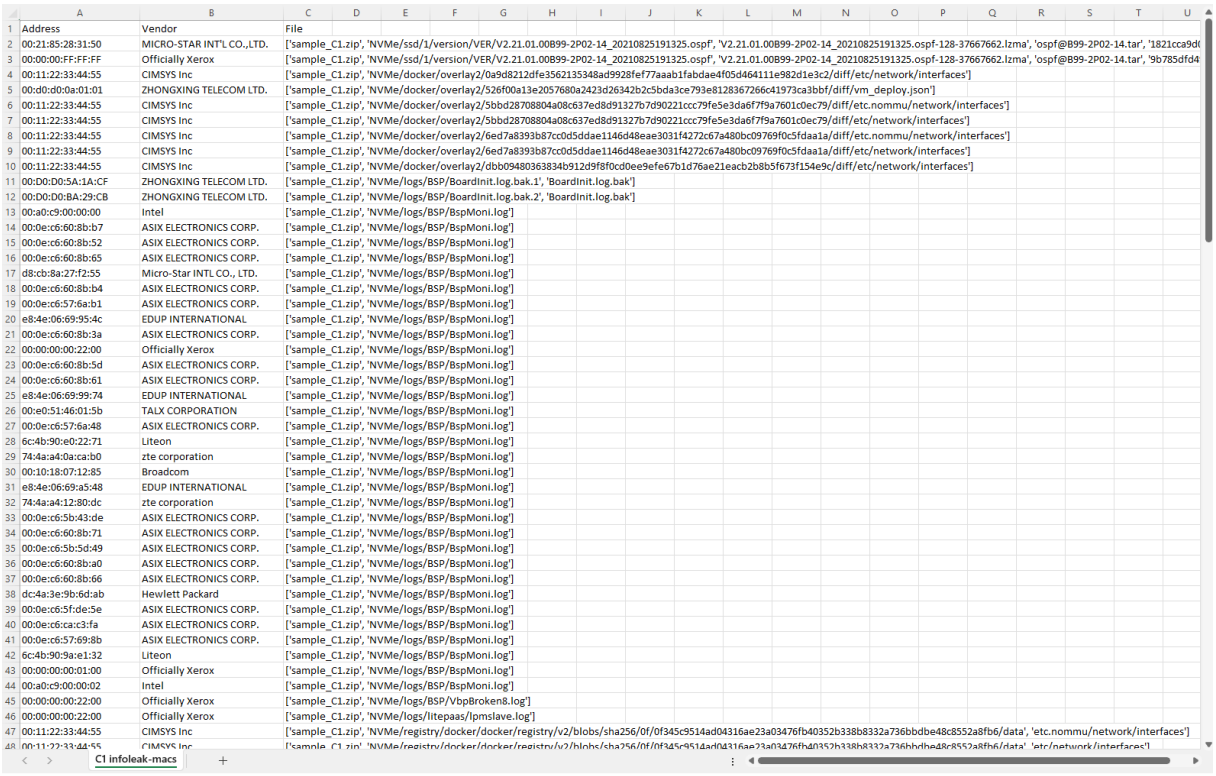
Figure 27: C1 Infoleak email addresses (Black Duck)



	A	B	C
1	IP	IPv6	File
2	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/006973cb603372590bd43086960e012b3bd54b61dbf8906eabf9a4871265997d/config.v2.json']
3	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/006973cb603372590bd43086960e012b3bd54b61dbf8906eabf9a4871265997d/config.v2.json']
4	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/006973cb603372590bd43086960e012b3bd54b61dbf8906eabf9a4871265997d/config.v2.json']
5	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/006973cb603372590bd43086960e012b3bd54b61dbf8906eabf9a4871265997d/config.v2.json']
6	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/00cf7a27cb921146ff9fcc91f259122adb66287d1c6dab2635ecf1881a8a099d/config.v2.json']
7	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/00cf7a27cb921146ff9fcc91f259122adb66287d1c6dab2635ecf1881a8a099d/config.v2.json']
8	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/00cf7a27cb921146ff9fcc91f259122adb66287d1c6dab2635ecf1881a8a099d/config.v2.json']
9	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/00cf7a27cb921146ff9fcc91f259122adb66287d1c6dab2635ecf1881a8a099d/config.v2.json']
10	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/02dc6f3b9ca935371226cbe7ccd8286a012544c6e09634066d00bf2f9f1c1b47/config.v2.json']
11	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/02dc6f3b9ca935371226cbe7ccd8286a012544c6e09634066d00bf2f9f1c1b47/config.v2.json']
12	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/02dc6f3b9ca935371226cbe7ccd8286a012544c6e09634066d00bf2f9f1c1b47/config.v2.json']
13	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/02dc6f3b9ca935371226cbe7ccd8286a012544c6e09634066d00bf2f9f1c1b47/config.v2.json']
14	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/04f0258734e2c96ee67dfc8c0f2e6901d5f427dc0cddb64330250be54455f005/config.v2.json']
15	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/04f0258734e2c96ee67dfc8c0f2e6901d5f427dc0cddb64330250be54455f005/config.v2.json']
16	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/04f0258734e2c96ee67dfc8c0f2e6901d5f427dc0cddb64330250be54455f005/config.v2.json']
17	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/04f0258734e2c96ee67dfc8c0f2e6901d5f427dc0cddb64330250be54455f005/config.v2.json']
18	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/07da92a05cb29830a4038437a2a3683b34f6ba7f8470cd37d98ce7f26c44af2d/config.v2.json']
19	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/07da92a05cb29830a4038437a2a3683b34f6ba7f8470cd37d98ce7f26c44af2d/config.v2.json']
20	127.0.0.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/07da92a05cb29830a4038437a2a3683b34f6ba7f8470cd37d98ce7f26c44af2d/hosts']
21	8.8.8.8	FALSE	['sample_C1.zip', 'NVMe/docker/containers/07da92a05cb29830a4038437a2a3683b34f6ba7f8470cd37d98ce7f26c44af2d/resolv.conf']
22	8.8.4.4	FALSE	['sample_C1.zip', 'NVMe/docker/containers/07da92a05cb29830a4038437a2a3683b34f6ba7f8470cd37d98ce7f26c44af2d/resolv.conf']
23	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0932600b4f5307744a7a1d35b2b37603cd767772dde04c2160e3d61fb5660573/config.v2.json']
24	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0932600b4f5307744a7a1d35b2b37603cd767772dde04c2160e3d61fb5660573/config.v2.json']
25	127.0.0.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0932600b4f5307744a7a1d35b2b37603cd767772dde04c2160e3d61fb5660573/hosts']
26	8.8.8.8	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0932600b4f5307744a7a1d35b2b37603cd767772dde04c2160e3d61fb5660573/resolv.conf']
27	8.8.4.4	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0932600b4f5307744a7a1d35b2b37603cd767772dde04c2160e3d61fb5660573/resolv.conf']
28	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f05c8855b1150485056e76ca9723306f0150c479b20124cc10b7cfd18baa74b/config.v2.json']
29	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f05c8855b1150485056e76ca9723306f0150c479b20124cc10b7cfd18baa74b/config.v2.json']
30	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f05c8855b1150485056e76ca9723306f0150c479b20124cc10b7cfd18baa74b/config.v2.json']
31	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f05c8855b1150485056e76ca9723306f0150c479b20124cc10b7cfd18baa74b/config.v2.json']
32	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f0ab7f9f0735f58e442e19f7023e575a6e5c8b60350c91fb91536b54029d07c/config.v2.json']
33	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f0ab7f9f0735f58e442e19f7023e575a6e5c8b60350c91fb91536b54029d07c/config.v2.json']
34	127.0.0.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f0ab7f9f0735f58e442e19f7023e575a6e5c8b60350c91fb91536b54029d07c/hosts']
35	8.8.8.8	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f0ab7f9f0735f58e442e19f7023e575a6e5c8b60350c91fb91536b54029d07c/resolv.conf']
36	8.8.4.4	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f0ab7f9f0735f58e442e19f7023e575a6e5c8b60350c91fb91536b54029d07c/resolv.conf']
37	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f55a6bc61a68c667a96230cf80bc42fd5d9589427a5b86b205e3ef8033a5570/config.v2.json']
38	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f55a6bc61a68c667a96230cf80bc42fd5d9589427a5b86b205e3ef8033a5570/config.v2.json']
39	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f55a6bc61a68c667a96230cf80bc42fd5d9589427a5b86b205e3ef8033a5570/config.v2.json']
40	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/0f55a6bc61a68c667a96230cf80bc42fd5d9589427a5b86b205e3ef8033a5570/config.v2.json']
41	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/101cfac99cd65d360e867aa366c6433c49a980e81a28af32ed895a8f3a3b8c73/config.v2.json']
42	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/101cfac99cd65d360e867aa366c6433c49a980e81a28af32ed895a8f3a3b8c73/config.v2.json']
43	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/101cfac99cd65d360e867aa366c6433c49a980e81a28af32ed895a8f3a3b8c73/config.v2.json']
44	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/101cfac99cd65d360e867aa366c6433c49a980e81a28af32ed895a8f3a3b8c73/config.v2.json']
45	192.254.1.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/10e4091610c5422a6f9f0407076e12202dec28e45fa2a9390269bbe2a4f17715/config.v2.json']
46	192.254.128.1	FALSE	['sample_C1.zip', 'NVMe/docker/containers/10e4091610c5422a6f9f0407076e12202dec28e45fa2a9390269bbe2a4f17715/config.v2.json']
47	173.254.128.2	FALSE	['sample_C1.zip', 'NVMe/docker/containers/10e4091610c5422a6f9f0407076e12202dec28e45fa2a9390269bbe2a4f17715/config.v2.json']
48	173.254.95.16	FALSE	['sample_C1.zip', 'NVMe/docker/containers/10e4091610c5422a6f9f0407076e12202dec28e45fa2a9390269bbe2a4f17715/config.v2.json']

C1 infoleak-ips

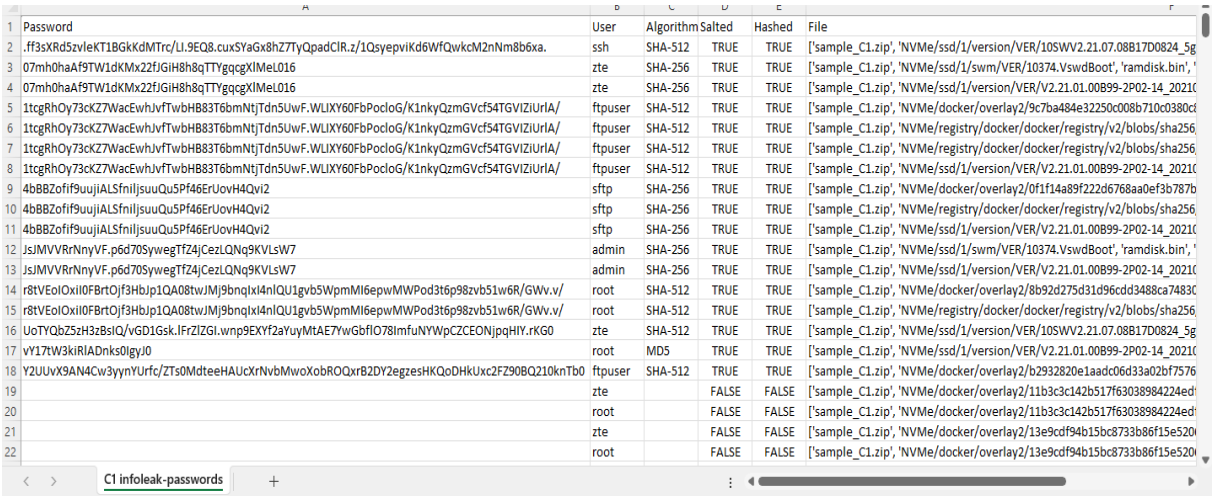
Figure 28: C1 Infoleak IP addresses (Black Duck)



Address	Vendor	File
00:21:85:28:31:50	MICRO-STAR INT'L CO.,LTD.	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210825191325.ospf', 'V2.21.01.00B99-2P02-14_20210825191325.ospf-128-37667662.lzma', 'ospf@B99-2P02-14.tar', '1821cca9d(
00:00:00:FF:FF:FF	Officially Xerox	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_20210825191325.ospf', 'V2.21.01.00B99-2P02-14_20210825191325.ospf-128-37667662.lzma', 'ospf@B99-2P02-14.tar', '9b785dfd4
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/etc/network/interfaces']
00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C1.zip', 'NVMe/docker/overlay2/526f00a13e2057680a2423d26342b2c5bda3ce793e8128367266c41973ca3bbf/diff/vm_deploy.json']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/docker/overlay2/5bbd28708804a08c637ed8d91327b7d90221ccc79fe5e3da6f7f9a7601c0ec79/diff/etc.nommu/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/docker/overlay2/5bbd28708804a08c637ed8d91327b7d90221ccc79fe5e3da6f7f9a7601c0ec79/diff/etc/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/docker/overlay2/6ed7a8393b87cc0d5ddae1146d48eae3031f4272c67a480bc09769f0c5fdaa1a/diff/etc.nommu/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/docker/overlay2/6ed7a8393b87cc0d5ddae1146d48eae3031f4272c67a480bc09769f0c5fdaa1a/diff/etc/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/docker/overlay2/dbb09480363834b912d9f8f0cd0ee9efe67b1d76ae21eacb2b8b5f673f154e9c/diff/etc/network/interfaces']
00:D0:D0:5A:1A:CF	ZHONGXING TELECOM LTD.	['sample_C1.zip', 'NVMe/logs/BSP/BoardInit.log.bak.1', 'BoardInit.log.bak']
00:D0:D0:BA:29:CB	ZHONGXING TELECOM LTD.	['sample_C1.zip', 'NVMe/logs/BSP/BoardInit.log.bak.2', 'BoardInit.log.bak']
00:a0:c9:00:00:00	Intel	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:b7	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:52	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:65	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
d8:cb:8a:27:f2:55	Micro-Star INTL CO., LTD.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:b4	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:57:6a:b1	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
e8:4e:06:69:95:4c	EDUP INTERNATIONAL	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:3a	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:00:00:00:22:00	Officially Xerox	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:5d	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:61	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
e8:4e:06:69:99:74	EDUP INTERNATIONAL	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:e0:51:46:01:5b	TALX CORPORATION	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:57:6a:48	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
6c:4b:90:e0:22:71	Liteon	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
74:4a:a4:0a:ca:b0	zte corporation	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:10:18:07:12:85	Broadcom	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
e8:4e:06:69:a5:48	EDUP INTERNATIONAL	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
74:4a:a4:12:80:dc	zte corporation	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:5b:43:de	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:71	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:5b:5d:49	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:a0	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:60:8b:66	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
dc:4a:3e:9b:6d:ab	Hewlett Packard	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:5f:de:5e	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:ca:c3:fa	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:0e:c6:57:69:8b	ASIX ELECTRONICS CORP.	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
6c:4b:90:9a:e1:32	Liteon	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:00:00:00:01:00	Officially Xerox	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:a0:c9:00:00:02	Intel	['sample_C1.zip', 'NVMe/logs/BSP/BspMoni.log']
00:00:00:00:22:00	Officially Xerox	['sample_C1.zip', 'NVMe/logs/BSP/VbpBroken8.log']
00:00:00:00:22:00	Officially Xerox	['sample_C1.zip', 'NVMe/logs/litepaas/lpmslave.log']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/0f/0f345c9514ad04316ae23a03476fb40352b338b8332a736bbdbe48c8552a8fb6/data', 'etc.nommu/network/interfaces']
00:11:22:33:44:55	CIMSYS Inc	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256/0f/0f345c9514ad04316ae23a03476fb40352b338b8332a736bbdbe48c8552a8fb6/data', 'etc/network/interfaces']

C1 infoleak-macs

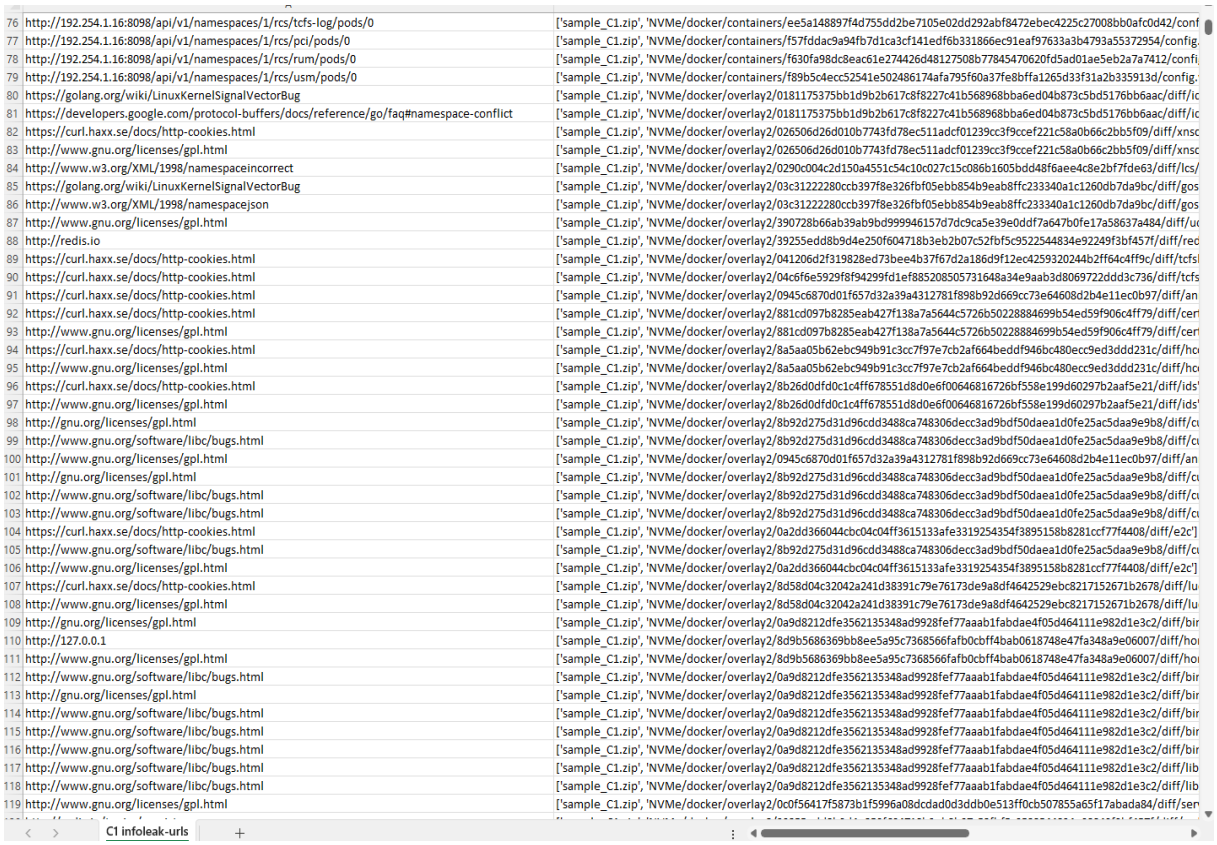
Figure 29: C1 Infoleak MAC addresses (Black Duck)



Password	User	Algorithm	Salted	Hashed	File
.ff3sXRd5zvIeKT1BGkKdMTrc/LI.9EQ8.cuxSYaGx8hZ7TyQpadClR.z/1QsyepviKd6WfQwkcM2nNm8b6xa.	ssh	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g
07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	zte	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', '
07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	zte	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_2021(
1tcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPoclo G/K1nkyQzmGVcf54TGVIZiUrlA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/9c7ba484e32250c008b710c0380c
1tcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPoclo G/K1nkyQzmGVcf54TGVIZiUrlA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
1tcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPoclo G/K1nkyQzmGVcf54TGVIZiUrlA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
1tcgRhOy73cKZ7WacEwhJvfTwbHB83T6bmNtjTdn5UwF.WLIXY60FbPoclo G/K1nkyQzmGVcf54TGVIZiUrlA/	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_2021(
4bBBZofif9uujiALSfniljsuuQu5Pf46ErUovH4Qvi2	sftp	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/0f1f14a89f222d6768aa0ef3b787b
4bBBZofif9uujiALSfniljsuuQu5Pf46ErUovH4Qvi2	sftp	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
4bBBZofif9uujiALSfniljsuuQu5Pf46ErUovH4Qvi2	sftp	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_2021(
JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', '
JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_2021(
r8tVEoIOxiI0FBrtOjf3HbJp1QA08twJMj9bnqIxI4nlQU1gvb5WpmMI6epwMWPod3t6p98zvb51w6R/GWv.v/	root	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca7483(
r8tVEoIOxiI0FBrtOjf3HbJp1QA08twJMj9bnqIxI4nlQU1gvb5WpmMI6epwMWPod3t6p98zvb51w6R/GWv.v/	root	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/registry/docker/docker/registry/v2/blobs/sha256
UoTYQbZ5zH3zBsIQ/vGD1Gsk.lFrZlZGI.wnp9EXYf2aYuyMtAE7YwGbfIO78ImfuNYWpCZCEONjpqHIY.rKG0	zte	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/10SWV2.21.07.08B17D0824_5g
vY17tW3kiRlADnks0lgyJ0	root	MD5	TRUE	TRUE	['sample_C1.zip', 'NVMe/ssd/1/version/VER/V2.21.01.00B99-2P02-14_2021(
Y2UUvX9AN4Cw3yynYUrfc/ZTs0MdteeHAUcXrNvbMwoXobROQxrB2DY2egzesHKQoDHkUxc2FZ90BQ210knTb0	ftpuser	SHA-512	TRUE	TRUE	['sample_C1.zip', 'NVMe/docker/overlay2/b2932820e1aadc06d33a02bf7576
	zte		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/11b3c3c142b517f63038984224ed
	root		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/11b3c3c142b517f63038984224ed
	zte		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/13e9cdf94b15bc8733b86f15e520
	root		FALSE	FALSE	['sample_C1.zip', 'NVMe/docker/overlay2/13e9cdf94b15bc8733b86f15e520

C1 infoleak-passwords

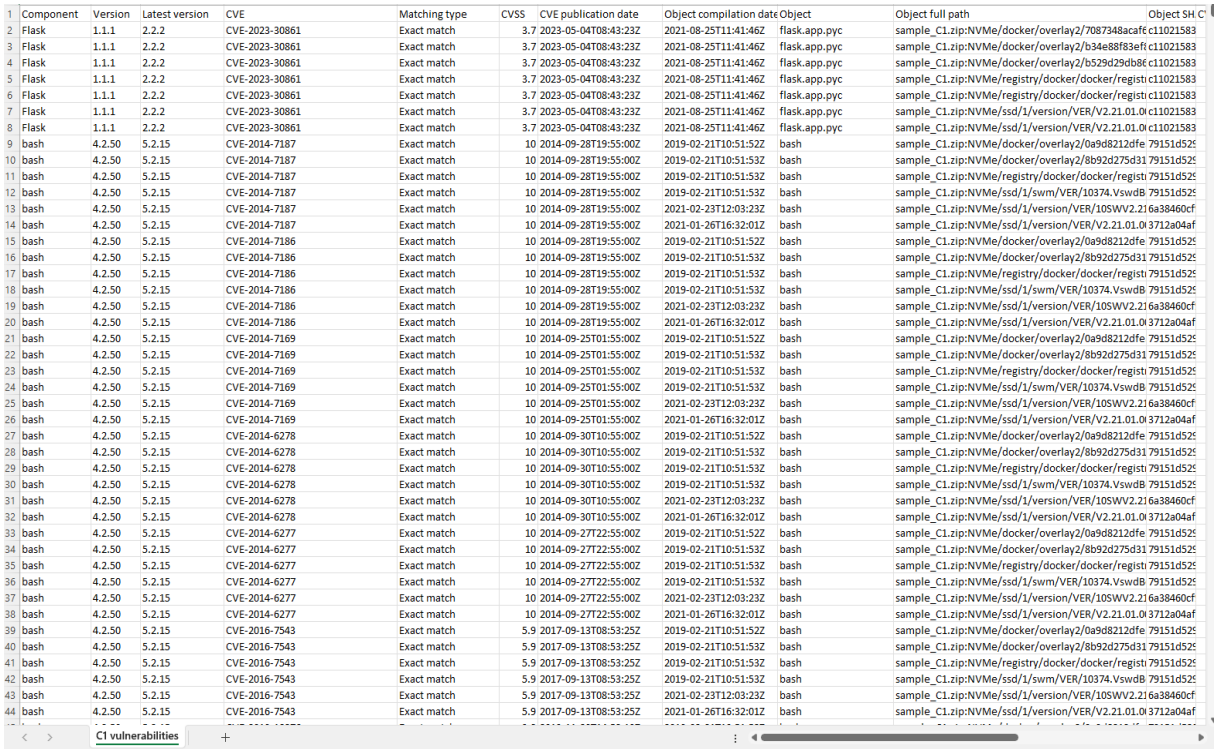
Figure 30: C1 Infoleak passwords (Black Duck)



76	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/tcfs-log/pods/0	['sample_C1.zip', 'NVMe/docker/containers/ee5a148897f4d755dd2be7105e02dd292abf8472ebec4225c27008bb0afc0d42/conf
77	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/pci/pods/0	['sample_C1.zip', 'NVMe/docker/containers/f57fddac9a94fb7d1ca3cf141edf6b331866ec91eaf97633a3b4793a55372954/config.
78	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/rum/pods/0	['sample_C1.zip', 'NVMe/docker/containers/f630fa98dc8eac61e274426d48127508b77845470620fd5ad01ae5eb2a7a7412/confi
79	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/usm/pods/0	['sample_C1.zip', 'NVMe/docker/containers/f89b5c4ecc52541e502486174afa795f60a37fe8bffa1265d33f31a2b335913d/config.
80	https://golang.org/wiki/LinuxKernelSignalVectorBug	['sample_C1.zip', 'NVMe/docker/overlay2/0181175375bb1d9b2b617c8f8227c41b568968bba6ed04b873c5bd5176bb6aac/diff/ic
81	https://developers.google.com/protocol-buffers/docs/reference/go/faq#namespace-conflict	['sample_C1.zip', 'NVMe/docker/overlay2/0181175375bb1d9b2b617c8f8227c41b568968bba6ed04b873c5bd5176bb6aac/diff/ic
82	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/026506d26d010b7743fd78ec511adcf01239cc3f9ccef221c58a0b66c2bb5f09/diff/xnsc
83	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/026506d26d010b7743fd78ec511adcf01239cc3f9ccef221c58a0b66c2bb5f09/diff/xnsc
84	http://www.w3.org/XML/1998/namespaceincorrect	['sample_C1.zip', 'NVMe/docker/overlay2/0290c004c2d150a4551c54c10c027c15c086b1605bdd48f6aee4c8e2bf7fde63/diff/lcs/
85	https://golang.org/wiki/LinuxKernelSignalVectorBug	['sample_C1.zip', 'NVMe/docker/overlay2/03c31222280ccb397f8e326fbf05ebb854b9eab8ffc233340a1c1260db7da9bc/diff/gos
86	http://www.w3.org/XML/1998/namespacejson	['sample_C1.zip', 'NVMe/docker/overlay2/03c31222280ccb397f8e326fbf05ebb854b9eab8ffc233340a1c1260db7da9bc/diff/gos
87	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/390728b66ab39ab9bd999946157d7dc9ca5e39e0ddf7a647b0fe17a58637a484/diff/uc
88	http://redis.io	['sample_C1.zip', 'NVMe/docker/overlay2/39255edd8b9d4e250f604718b3eb2b07c52fbf5c9522544834e92249f3bf457f/diff/rec
89	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/041206d2f319828ed73bee4b37f67d2a186d9f12ec4259320244b2ff64c4ff9c/diff/tcfs
90	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/04c6f6e5929f8f94299fd1ef885208505731648a34e9aab3d8069722ddd3c736/diff/tcfs
91	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/0945c6870d01f657d32a39a4312781f898b92d669cc73e64608d2b4e11ec0b97/diff/an
92	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/881cd097b8285eab427f138a7a5644c5726b50228884699b54ed59f906c4ff79/diff/cer
93	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/881cd097b8285eab427f138a7a5644c5726b50228884699b54ed59f906c4ff79/diff/cer
94	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/8a5aa05b62ebc949b91c3cc7f97e7cb2af664beddf946bc480ecc9ed3ddd231c/diff/hc
95	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8a5aa05b62ebc949b91c3cc7f97e7cb2af664beddf946bc480ecc9ed3ddd231c/diff/hc
96	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b26d0dfd0c1c4ff678551d8d0e6f00646816726bf558e199d60297b2aaf5e21/diff/ids'
97	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b26d0dfd0c1c4ff678551d8d0e6f00646816726bf558e199d60297b2aaf5e21/diff/ids'
98	http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/cu
99	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/cu
100	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0945c6870d01f657d32a39a4312781f898b92d669cc73e64608d2b4e11ec0b97/diff/an
101	http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/cu
102	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/cu
103	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/cu
104	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a2dd366044cbc04c04ff3615133afe3319254354f3895158b8281ccf77f4408/diff/e2c']
105	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/8b92d275d31d96cdd3488ca748306decc3ad9bdf50daea1d0fe25ac5daa9e9b8/diff/cu
106	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a2dd366044cbc04c04ff3615133afe3319254354f3895158b8281ccf77f4408/diff/e2c']
107	https://curl.haxx.se/docs/http-cookies.html	['sample_C1.zip', 'NVMe/docker/overlay2/8d58d04c32042a241d38391c79e76173de9a8df4642529ebc8217152671b2678/diff/lu
108	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8d58d04c32042a241d38391c79e76173de9a8df4642529ebc8217152671b2678/diff/lu
109	http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bir
110	http://127.0.0.1	['sample_C1.zip', 'NVMe/docker/overlay2/8d9b5686369bb8ee5a95c7368566fafb0cbff4bab0618748e47fa348a9e06007/diff/ho
111	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/8d9b5686369bb8ee5a95c7368566fafb0cbff4bab0618748e47fa348a9e06007/diff/ho
112	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bir
113	http://gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bir
114	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bir
115	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bir
116	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/bir
117	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/lib
118	http://www.gnu.org/software/libc/bugs.html	['sample_C1.zip', 'NVMe/docker/overlay2/0a9d8212dfe3562135348ad9928fef77aaab1fabdae4f05d464111e982d1e3c2/diff/lib
119	http://www.gnu.org/licenses/gpl.html	['sample_C1.zip', 'NVMe/docker/overlay2/0c0f56417f5873b1f5996a08dcdad0d3ddb0e513ff0cb507855a65f17abada84/diff/ser

C1 infoleak-urls

Figure 31: C1 Infoleak URLs (Black Duck)



	Component	Version	Latest version	CVE	Matching type	CVSS	CVE publication date	Object compilation date	Object	Object full path	Object SH C
2	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/overlay2/7087348acafc	c11021583
3	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/b34e88f83efc	c11021583
4	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/b529d29db8f	c11021583
5	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/registi	c11021583
6	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/registi	c11021583
7	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	c11021583
8	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	c11021583
9	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	79151d525
10	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/overlay2/8b92d275d31	79151d525
11	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/registi	79151d525
12	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	79151d525
13	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/10SWV2.216a38460cf	
14	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	3712a04af
15	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	79151d525
16	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/overlay2/8b92d275d31	79151d525
17	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	79151d525
18	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	79151d525
19	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/10SWV2.216a38460cf	
20	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	3712a04af
21	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	79151d525
22	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/overlay2/8b92d275d31	79151d525
23	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	79151d525
24	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	79151d525
25	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/10SWV2.216a38460cf	
26	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	3712a04af
27	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	79151d525
28	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/overlay2/8b92d275d31	79151d525
29	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	79151d525
30	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	79151d525
31	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/10SWV2.216a38460cf	
32	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	3712a04af
33	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	79151d525
34	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/overlay2/8b92d275d31	79151d525
35	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	79151d525
36	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	79151d525
37	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/10SWV2.216a38460cf	
38	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	3712a04af
39	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	79151d525
40	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/overlay2/8b92d275d31	79151d525
41	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/registi	79151d525
42	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	79151d525
43	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/10SWV2.216a38460cf	
44	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	3712a04af

C1 vulnerabilities

Figure 32: C1 CVEs (Black Duck)

Sample C1 Code Sentry Scan Report Excerpts

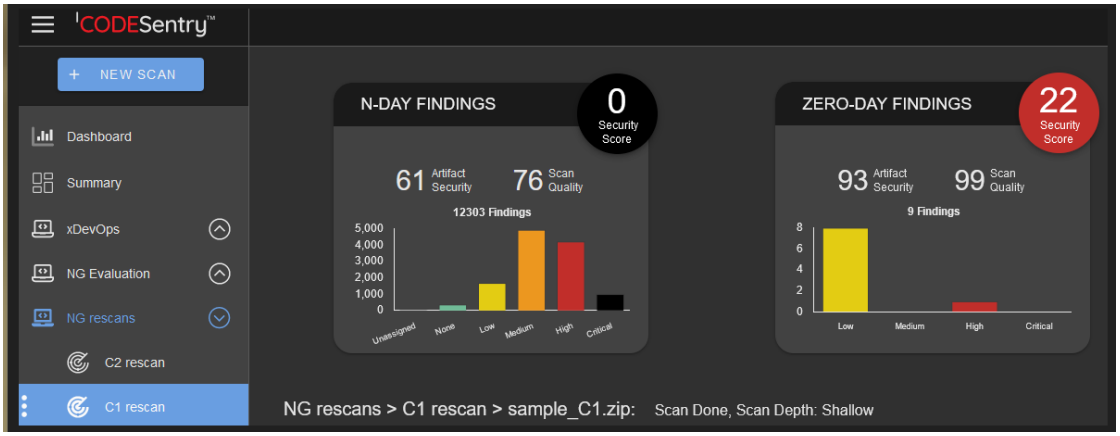


Figure 33: C1 Scan Overview (Code Sentry)

GRAMMATECH CODESentry

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/d6b78809c7d314892e2e768caf6c36b61160cc0fc3f6904118b2eba9e08ac97a/diff/lib/libadlik_serving.so
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/244d5830ec9dad40a01c0c38b85bd20bd5c85fa08c6fe5ff1d2d25e852fdc2b4/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/244d5830ec9dad40a01c0c38b85bd20bd5c85fa08c6fe5ff1d2d25e852fdc2b4/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/2af8e33e510b55ae4eda6cf1b8941b01e12e990961e366011a7da4ece862280b/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/2af8e33e510b55ae4eda6cf1b8941b01e12e990961e366011a7da4ece862280b/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/67c1e05171180bb47a8cdb284e1d0ab0a1ee20a287d890d179406d4328f8d892/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/9c7ba484e32250c008b710c0380c8e7cc76d0938ea67279dabad0a0bfdfa1be1/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/9c7ba484e32250c008b710c0380c8e7cc76d0938ea67279dabad0a0bfdfa1be1/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/a4ab53eb37cd01459ddef42225a56e60020d4dc204a486aeded3f9fc8505171b/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/a7b441174f8dca161986724cec4ab9db39d21b3bf1569637220e6da984c576a3/diff/ordinaryuserhome/setfacl

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

GRAMMATECH CODESentry

N-Day Findings

Findings for sample_C1.zip

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

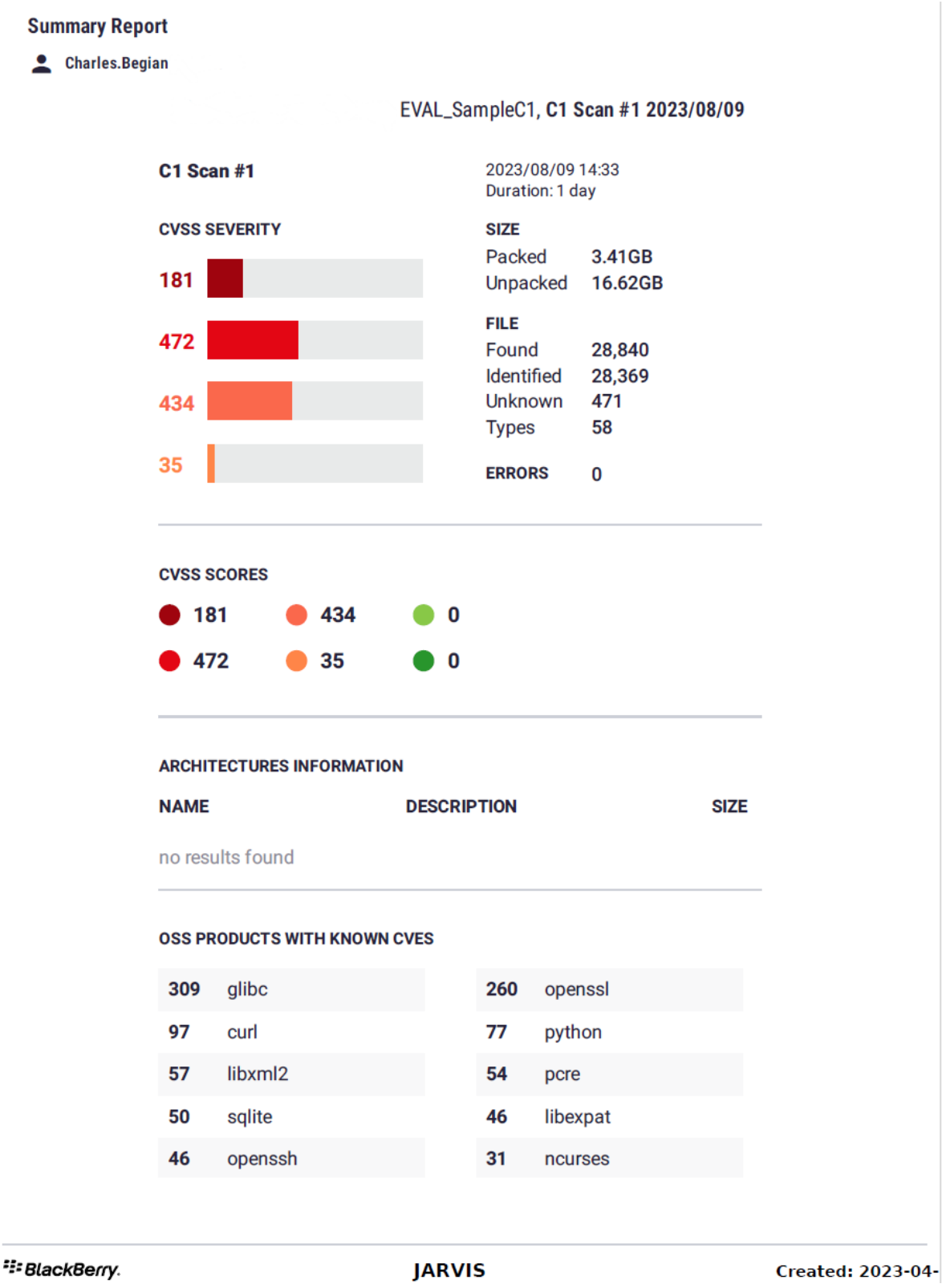
linux [unspecified] 2.4.20-wolk4.14-fullkernel

Match Level: **Low**
Security Score: **0**
Path: **NG rescans/C1 rescan/sample_C1.zip/NVMe/docker/overlay2/5292f87836e697470edcfe706a689df0ae2d15abe3ff91f97df7b24fa6395228/diff/pcs.exe**
Component ID: 48373a2d-9959-47f9-a5ca-7c707aa4930d
Score Distribution: Unassigned: 0 None: 26 Low: 262 Medium: 799 High: 456 Critical: 32

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	252698	Linux Kernel fs/f2fs/node.c get_next_net_page() Functio...
Critical	9.8	3.0	262402	Linux Kernel drivers/net/usb/hso.c hso_free_net_device(...
Critical	9.8	3.0	274228	Linux Kernel fs/nfsd/nfs4xdr.c nfsd4_decode_bitmap4() F...

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

Sample C1 Jarvis Scan Report Excerpts



Summary Report

Charles.Begian

EVAL_SampleC1, **C1 Scan #1 2023/08/09**

C1 Scan #1

2023/08/09 14:33
Duration: 1 day

CVSS SEVERITY

181
472
434
35

SIZE

Packed	3.41GB
Unpacked	16.62GB

FILE

Found	28,840
Identified	28,369
Unknown	471
Types	58

ERRORS 0

CVSS SCORES

181	434	0
472	35	0

ARCHITECTURES INFORMATION

NAME	DESCRIPTION	SIZE
no results found		

OSS PRODUCTS WITH KNOWN CVES

309	glibc	260	openssl
97	curl	77	python
57	libxml2	54	pcre
50	sqlite	46	libexpat
46	openssh	31	ncurses

BlackBerry. JARVIS Created: 2023-04-

Figure 36: C1 Scan Overview (Jarvis)

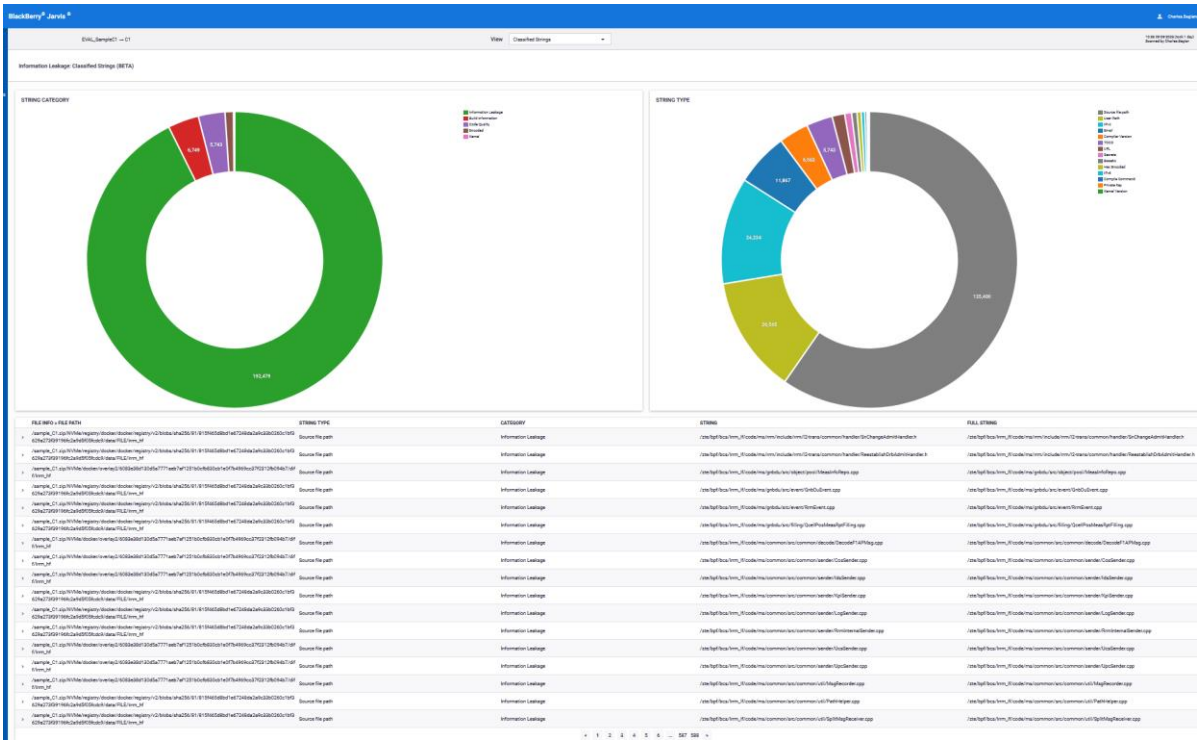


Figure 37: C1 Information Leakage (Jarvis)

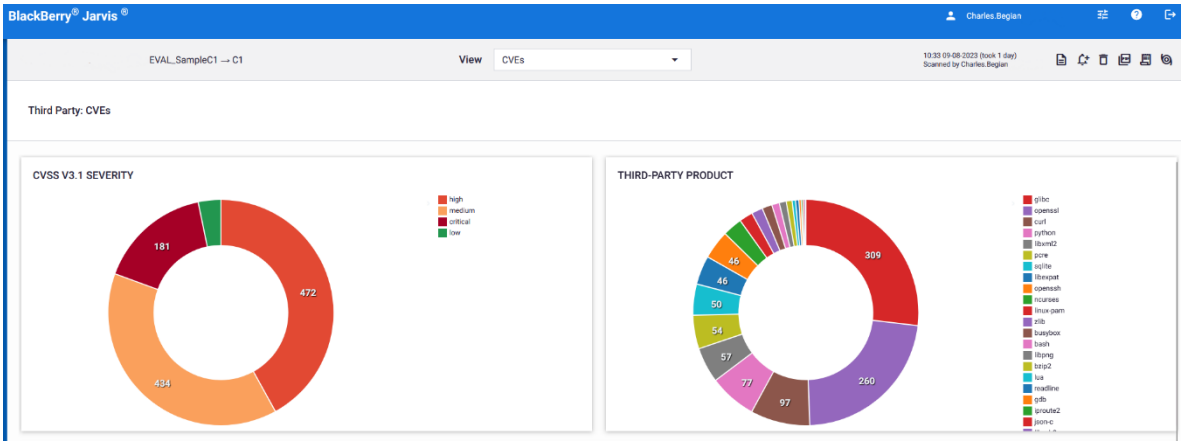


Figure 38: CVSS Severity Report (Jarvis)

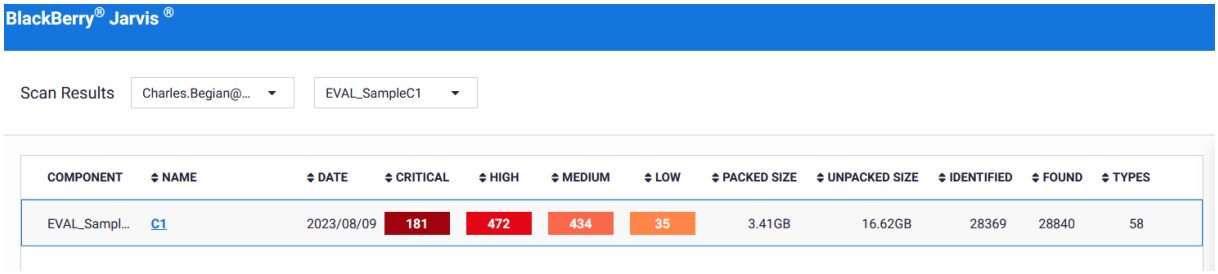
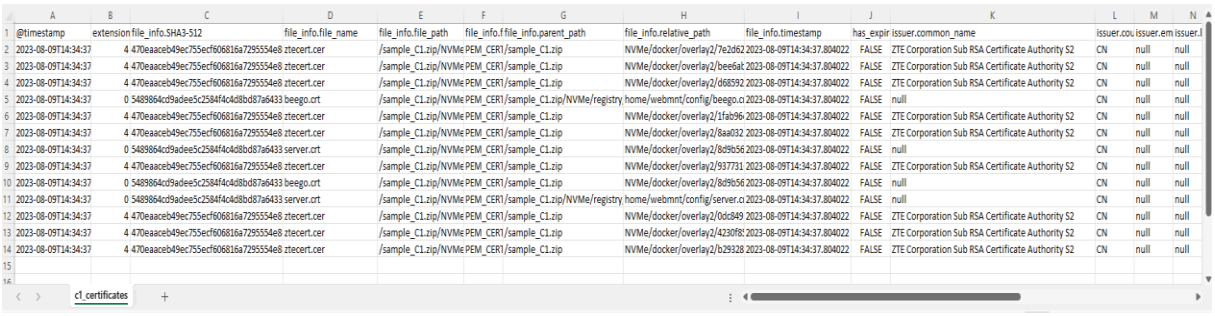


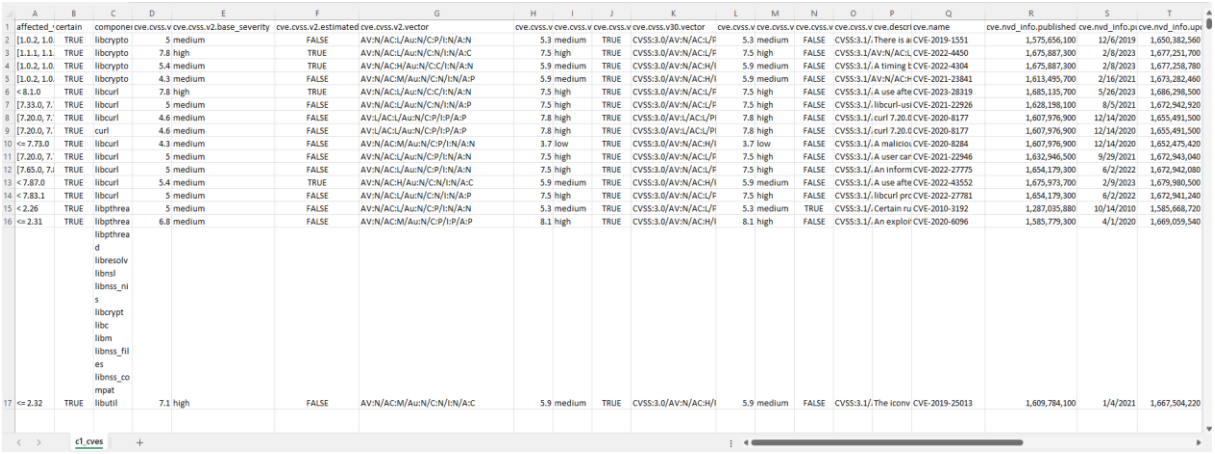
Figure 39: CVE Summary by Severity (Jarvis)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	@timestamp	extension	file_info.SHA3-512	file_info.file_name	file_info.file_path	file_info.f	file_info.parent_path	file_info.relative_path	file_info.timestamp	has_expir	issuer.common_name	issuer.cou	issuer.em	issuer.l
2	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
3	2023-08-09T14:34:37	4	470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1	/sample_C1.zip	NVMe/docker/overlay2/bee6a8	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
4	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
5	2023-08-09T14:34:37	0	5489864cd9adee5c2584f4c4d8bd87a6433	beego.crt	/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
6	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
7	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
8	2023-08-09T14:34:37	0	5489864cd9adee5c2584f4c4d8bd87a6433	server.crt	/sample_C1.zip/NVMe	PEM_CER1	/sample_C1.zip	NVMe/docker/overlay2/8d9b56	2023-08-09T14:34:37.804022	FALSE	null	CN	null	null
9	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
10	2023-08-09T14:34:37	0	5489864cd9adee5c2584f4c4d8bd87a6433	beego.crt	/sample_C1.zip/NVMe	PEM_CER1	/sample_C1.zip	NVMe/docker/overlay2/8d9b56	2023-08-09T14:34:37.804022	FALSE	null	CN	null	null
11	2023-08-09T14:34:37	0	5489864cd9adee5c2584f4c4d8bd87a6433	server.crt	/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
12	2023-08-09T14:34:37	4	470eaaceb49ec755ecf606816a7295554e8	ztecert.cer	/sample_C1.zip/NVMe	PEM_CER1	/sample_C1.zip	NVMe/docker/overlay2/0dc949	2023-08-09T14:34:37.804022	FALSE	ZTE Corporation Sub RSA Certificate Authority S2	CN	null	null
13	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
14	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
15														
16														

c1_certificates

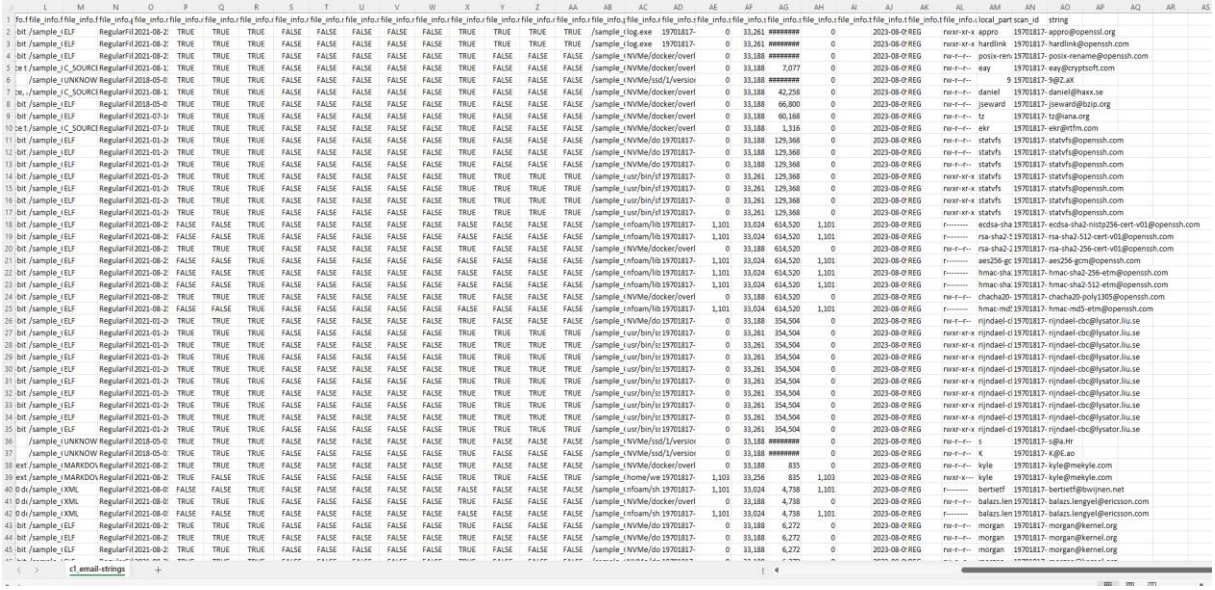
Figure 40: C1 Certificates report (Jarvis)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	affected_	certain	componer	cve.cvss.v	cve.cvss.v2.base_severity	cve.cvss.v2.estimated	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.descri	cve.name	cve.nvd_info.published	cve.nvd_info.p	cve.nvd_info.up
2	[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/F	5.3	medium	FALSE	CVSS:3.1/	There is a	CVE-2019-1551	1,575,656,100	12/6/2019	1,650,382,560
3	[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/F	7.5	high	FALSE	CVSS:3.1/	AV:N/AC:L	CVE-2022-4450	1,675,887,300	2/8/2023	1,677,251,700
4	[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/	A timing t	CVE-2022-4304	1,675,887,300	2/8/2023	1,677,258,780
5	[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	1,673,282,460
6	< 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/F	7.5	high	FALSE	CVSS:3.1/	A use afte	CVE-2023-28319	1,685,135,700	5/26/2023	1,686,298,500
7	[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/F	7.5	high	FALSE	CVSS:3.1/	libcurl-usi	CVE-2021-22926	1,628,198,100	8/5/2021	1,672,942,920
8	[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	1,655,491,500
9	[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	1,655,491,500
10	<= 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	1,652,475,420
11	[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/F	7.5	high	FALSE	CVSS:3.1/	A user can	CVE-2021-22946	1,632,946,500	9/29/2021	1,672,943,040
12	[7.65.0, 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/F	7.5	high	FALSE	CVSS:3.1/	An inform	CVE-2022-27775	1,654,179,300	6/2/2022	1,672,942,080
13	< 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 afte	CVE-2022-43552	1,675,973,700	2/9/2023	1,679,980,500
14	< 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/F	7.5	high	FALSE	CVSS:3.1/	libcurl prc	CVE-2022-27781	1,654,179,300	6/2/2022	1,672,941,240
15	< 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/F	5.3	medium	TRUE	CVSS:3.1/	Certain ru	CVE-2010-3192	1,287,035,880	10/14/2010	1,585,668,720
16	<= 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 explois	CVE-2020-6096	1,585,779,300	4/1/2020	1,669,059,540
			libpthrea d libresolv libnsl libnss_ni s libcrypt libc libm libnss_fil es libnss_co mpat																	
17	<= 2.32	TRUE	libutil	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/I	5.9	medium	FALSE	CVSS:3.1/	The iconv	CVE-2019-25013	1,609,784,100	1/4/2021	1,667,504,220

c1_cves

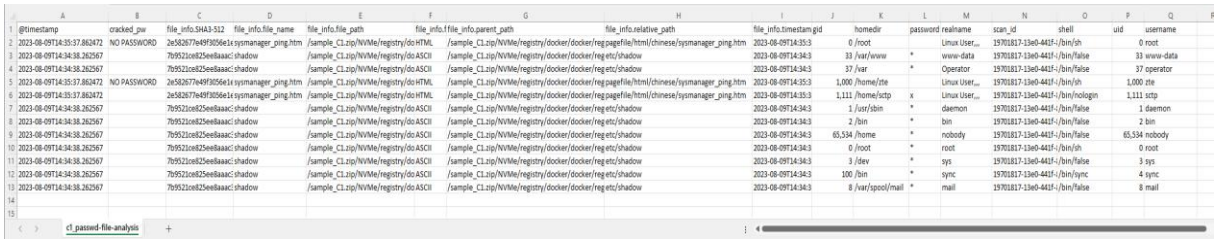
Figure 41: C1 CVEs (Jarvis)



	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS
1	fo.file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	file_info.f	local_part	scan_id	string					
2	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	log.exe	19701817-	0	33,261	########	0		2023-08-0	REG	rwxr-xr-x	appro	19701817-	appro@openssl.org				
3	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	log.exe	19701817-	0	33,261	########	0		2023-08-0	REG	rwxr-xr-x	hardlink	19701817-	hardlink@openssh.com				
4	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	########	0		2023-08-0	REG	rw-r--r--	posix-ren	19701817-	posix-rename@openssh.com				
5	ze /sample_(	C_SOURCI	Regular Fil	2021-08-1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	7,077	0		2023-08-0	REG	rw-r--r--	eay	19701817-	eay@cryptsoft.com				
6	/sample_(	UNKNOW	Regular Fil	2018-05-0	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/ssd/1/versio		0	33,188	########	0		2023-08-0	REG	rw-r--r--		9	19701817-	s@2.at				
7	ze, /sample_(	C_SOURCI	Regular Fil	2021-08-1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	42,258	0		2023-08-0	REG	rw-r--r--	daniel	19701817-	daniel@haxx.se				
8	bit /sample_(	ELF	Regular Fil	2018-05-0	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	66,800	0		2023-08-0	REG	rw-r--r--	jseward	19701817-	jseward@bzip.org				
9	bit /sample_(	ELF	Regular Fil	2021-07-1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	60,168	0		2023-08-0	REG	rw-r--r--	tz	19701817-	tz@iana.org				
10	ze /sample_(	C_SOURCI	Regular Fil	2021-07-1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	1,316	0		2023-08-0	REG	rw-r--r--	ekr	19701817-	ekr@rtfm.com				
11	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	129,368	0		2023-08-0	REG	rw-r--r--	statvfs	19701817-	statvfs@openssh.com				
12	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	129,368	0		2023-08-0	REG	rw-r--r--	statvfs	19701817-	statvfs@openssh.com				
13	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	129,368	0		2023-08-0	REG	rw-r--r--	statvfs	19701817-	statvfs@openssh.com				
14	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	129,368	0		2023-08-0	REG	rwxr-xr-x	statvfs	19701817-	statvfs@openssh.com				
15	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	129,368	0		2023-08-0	REG	rwxr-xr-x	statvfs	19701817-	statvfs@openssh.com				
16	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	129,368	0		2023-08-0	REG	rwxr-xr-x	statvfs	19701817-	statvfs@openssh.com				
17	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	129,368	0		2023-08-0	REG	rwxr-xr-x	statvfs	19701817-	statvfs@openssh.com				
18	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	ecdsa-sha	19701817-	ecdsa-sha2-nistp256-cert-v01@openssh.com				
19	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	rsa-sha2-2	19701817-	rsa-sha2-512-cert-v01@openssh.com				
20	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	rsa-sha2-2	19701817-	rsa-sha2-256-cert-v01@openssh.com				
21	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	aes256-gc	19701817-	aes256-gcm@openssh.com				
22	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	hmac-sha	19701817-	hmac-sha2-256-etm@openssh.com				
23	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	hmac-sha	19701817-	hmac-sha2-512-etm@openssh.com				
24	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	614,520	0		2023-08-0	REG	rw-r--r--	chacha20-	19701817-	chacha20-poly1305@openssh.com				
25	bit /sample_(	ELF	Regular Fil	2021-08-2	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/lib	19701817-	1,101	33,024	614,520	1,101		2023-08-0	REG	r---------	hmac-md5	19701817-	hmac-md5-etm@openssh.com				
26	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	354,504	0		2023-08-0	REG	rw-r--r--	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
27	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
28	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
29	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
30	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
31	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
32	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
33	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
34	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
35	bit /sample_(	ELF	Regular Fil	2021-01-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	/sample_(	usr/bin/sf	19701817-	0	33,261	354,504	0		2023-08-0	REG	rwxr-xr-x	rijndael-cl	19701817-	rijndael-cbc@lysator.liu.se				
36		/sample_(	UNKNOW	Regular Fil	2018-05-0	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/ssd/1/versio		0	33,188	########	0		2023-08-0	REG	rw-r--r--	s	19701817-	s@a.Hr				
37		/sample_(	UNKNOW	Regular Fil	2018-05-0	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/ssd/1/versio		0	33,188	########	0		2023-08-0	REG	rw-r--r--	K	19701817-	K@E.ao				
38	ext /sample_(	MARKDO	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	835	0		2023-08-0	REG	rw-r--r--	kyle	19701817-	kyle@mekyle.com				
39	ext /sample_(	MARKDO	Regular Fil	2021-08-2	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE	/sample_(	home/swe	19701817-	1,103	33,256	835	1,103		2023-08-0	REG	rwxr-x---	kyle	19701817-	kyle@mekyle.com				
40	0 ds /sample_(	XML	Regular Fil	2021-08-0	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/sh	19701817-	1,101	33,024	4,738	1,101		2023-08-0	REG	r---------	bertietf	19701817-	bertietf@bwijnen.net				
41	0 ds /sample_(	XML	Regular Fil	2021-08-0	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	NVMe/docker/overl		0	33,188	4,738	0		2023-08-0	REG	rw-r--r--	balazs.len	19701817-	balazs.lengyel@ericsson.com				
42	0 ds /sample_(	XML	Regular Fil	2021-08-0	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	/sample_(	nfoam/sh	19701817-	1,101	33,024	4,738	1,101		2023-08-0	REG	r---------	balazs.len	19701817-	balazs.lengyel@ericsson.com				
43	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	6,272	0		2023-08-0	REG	rw-r--r--	morgan	19701817-	morgan@kernel.org				
44	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	6,272	0		2023-08-0	REG	rw-r--r--	morgan	19701817-	morgan@kernel.org				
45	bit /sample_(	ELF	Regular Fil	2021-08-2	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	/sample_(	NVMe/do	19701817-	0	33,188	6,272	0		2023-08-0	REG	rw-r--r--	morgan	19701817-	morgan@kernel.org				

c1_email-strings

Figure 42: C1 email addresses (Jarvis)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	@timestamp	cracked_pw	file_info.SHA3-512	file_info.file_name	file_info.file_path	file_info.f	file_info.parent_path	file_info.relative_path	file_info.timestam	gid	homedir	password	realname	scan_id	shell	uid	username
2	2023-08-09T14:35:37.862472	NO PASSWORD	2e582677e49f3056e1e	sysmanager_ping.htm	/sample_C1.zip/NVMe/registry/do	HTML	/sample_C1.zip/NVMe/registry/docker/docker/reg	pagefile/html/chinese/sysmanager_ping.htm	2023-08-09T14:35:3		0 /root		Linux User,,,	19701817-13e0-441f-	/bin/sh	0	root
3	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		33 /var/www	*	www-data	19701817-13e0-441f-	/bin/false	33	www-data
4	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		37 /var	*	Operator	19701817-13e0-441f-	/bin/false	37	operator
5	2023-08-09T14:35:37.862472	NO PASSWORD	2e582677e49f3056e1e	sysmanager_ping.htm	/sample_C1.zip/NVMe/registry/do	HTML	/sample_C1.zip/NVMe/registry/docker/docker/reg	pagefile/html/chinese/sysmanager_ping.htm	2023-08-09T14:35:3		1,000 /home/zte		Linux User,,,	19701817-13e0-441f-	/bin/sh	1,000	zte
6	2023-08-09T14:35:37.862472		2e582677e49f3056e1e	sysmanager_ping.htm	/sample_C1.zip/NVMe/registry/do	HTML	/sample_C1.zip/NVMe/registry/docker/docker/reg	pagefile/html/chinese/sysmanager_ping.htm	2023-08-09T14:35:3		1,111 /home/sctp	x	Linux User,,,	19701817-13e0-441f-	/bin/nologin	1,111	sctp
7	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		1 /usr/sbin	*	daemon	19701817-13e0-441f-	/bin/false	1	daemon
8	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		2 /bin	*	bin	19701817-13e0-441f-	/bin/false	2	bin
9	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3	65,534	/home	*	nobody	19701817-13e0-441f-	/bin/false	65,534	nobody
10	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		0 /root	*	root	19701817-13e0-441f-	/bin/sh	0	root
11	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		3 /dev	*	sys	19701817-13e0-441f-	/bin/false	3	sys
12	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		100 /bin	*	sync	19701817-13e0-441f-	/bin/sync	4	sync
13	2023-08-09T14:34:38.262567		7b9521ce825ee8aaac	shadow	/sample_C1.zip/NVMe/registry/do	ASCII	/sample_C1.zip/NVMe/registry/docker/docker/reg	etc/shadow	2023-08-09T14:34:3		8 /var/spool/mail	*	mail	19701817-13e0-441f-	/bin/false	8	mail
14																	
15																	

c1_passwd-file-analysis +

Figure 43: C1 Password File Analysis (Jarvis)

	file_info.extension	file_info.file_name	file_info.file_output	file_info.file_path	file_info.file_type	file_info.groups	file_info	fragment	netloc	path	query	scheme	string	file_info.scan_id
2	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/docker/ov	JAVASCRIPT	RegularFile, Executable	REG		schemas.openxmlformat	/officeDocument/2006/relationships/officeDocument	",SHEET:"ht	http	http://schemas.openxmlformats.org/officeDocument/2006/rel	
3	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG		purl.org	/dc/elements/1.1		http	http://pur	19701817-13e0-441f-8512-df2fc0569de0
4	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG		schemas.openxmlformat	/officeDocument/2006/custom-properties",Kn.CUST_PROPS="htt		http	http://schemas.openxmlformats.org/officeDocument/2006/cu	
5	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG		schemas.openxmlformat	/officeDocument/2006/relationships/theme"		http	http://schemas.openxmlformats.org/officeDocument/2006/rel	
6	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG		schemas.openxmlformat	/officeDocument/2006/relationships/worksheet","http://purl.oclhttp		http	http://sch	19701817-13e0-441f-8512-df2fc0569de0
7	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG		"","xmlns:tableooo"="ht purl.org			http		19701817-13e0-441f-8512-df2fc0569de0
8	.js	14.56b243b036f056b79c68.js	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG		docs.oasis-open.org	/ns/office/1.2/meta/pkg		http	http://docs.oasis-open.org/ns/office/1.2/meta/pkg	
9	.exe	log.exe	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		www.baidu.com			<none>	www.baidu.com	
10	.exe	log.exe	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/registry/dc	ELF	RegularFile, Executable	REG		www.baidu.com			<none>	www.baic	19701817-13e0-441f-8512-df2fc0569de0
11		lrrm_hf	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/registry/dc	ELF	RegularFile, Executable	REG		curl.haxx.se	/docs/http-cookies.html		https	https://cu	19701817-13e0-441f-8512-df2fc0569de0
12	.ttf	opensans.ttf	TrueType Font data, digitally signed, 19 tables, 1st "DSI	/sample_C1.zip/NVMe/docker/ov	TTF	RegularFile, Font, Non	REG		www.ascendercorp.com	/http://www.ascendercorp.com/typedesigners.html,Licensed		http	http://www.ascendercorp.com/http://www.ascendercorp.com	
13	.ttf	opensans.ttf	TrueType Font data, digitally signed, 19 tables, 1st "DSI	/sample_C1.zip/NVMe/registry/dc	TTF	RegularFile, Font, Non	REG		www.verisign.com	/rpa		https	https://www.verisign.com/rpa	
14	.ttf	opensans.ttf	TrueType Font data, digitally signed, 19 tables, 1st "DSI	/sample_C1.zip/NVMe/registry/dc	TTF	RegularFile, Font, Non	REG		logo.verisign.com	/vslogo.gif0		http	http://logo.verisign.com/vslogo.gif0	
15	.h	typecheck-gcc.h	C source, ASCII text	/sample_C1.zip/NVMe/docker/ov	C_SOURCE	RegularFile, Sourcecod	REG		curl.haxx.se	/docs/copyright.html		https	https://curl.haxx.se/docs/copyright.html	
16	.h	typecheck-gcc.h	C source, ASCII text	/sample_C1.zip/NVMe/registry/dc	C_SOURCE	RegularFile, Sourcecod	REG		curl.haxx.se	/docs/copyright.html		https	https://cu	19701817-13e0-441f-8512-df2fc0569de0
17	.svg	import_xml120.svg	SVG Scalable Vector Graphics image	/sample_C1.zip/NVMe/registry/dc	SVG	RegularFile, Image, Non	REG		www.bohemiancoding.cc	/sketch		http	http://ww	19701817-13e0-441f-8512-df2fc0569de0
18		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		curl.se	/libcurl/c/curl_easy_setopt.html		https	https://curl.se/libcurl/c/curl_easy_setopt.html	
19		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		example.com	/file[1-100:10].txt		http	http://example.com/file[1-100:10].txt	
20		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		curl.se	/docs		https	https://curl.se/docs	
21		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/registry/dc	ELF	RegularFile, Executable	REG		nowhereatall.example.com			https	https://no	19701817-13e0-441f-8512-df2fc0569de0
22		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		curl.se	/docs/sslcerts.html		https	https://curl.se/docs/sslcerts.html	
23		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/registry/dc	ELF	RegularFile, Executable	REG		curl.se	/docs/sslcerts.html		https	https://cu	19701817-13e0-441f-8512-df2fc0569de0
24		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		www.notlocal.com			<none>	www.notlocal.com	
25	.md	readme.md	ASCII text	/sample_C1.zip/NVMe/docker/ov	MARKDOWN	RegularFile, Document	REG		scripts.sil.org	/OFL		http	http://scripts.sil.org/OFL	
26	.eot	iconfont.eot	Embedded OpenType (EOT), iconfont family	/sample_C1.zip/NVMe/docker/ov	EOT	RegularFile, Font, Non	REG		fontello.com			http	http://fontello.com	
27	.yin	ietf-netconf-with-defaults.yin	XML 1.0 document text	/sample_C1.zip/NVMe/registry/dc	XML	RegularFile, Markup, N	REG		trustee.ietf.org	/license-info		http	http://tru	19701817-13e0-441f-8512-df2fc0569de0
28	.svg	Error.svg	SVG Scalable Vector Graphics image	/sample_C1.zip/NVMe/registry/dc	SVG	RegularFile, Image, Non	REG		sketchapp.com			https	https://sk	19701817-13e0-441f-8512-df2fc0569de0
29	.js	vendor.b9b044bbd3e0c69b9c7	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/docker/ov	JAVASCRIPT	RegularFile, Executable	REG	/zh-CN/component/up	element.eleme.io	/		http	http://element.eleme.io/#/zh-CN/component/upload#yong-h	
30	.js	vendor.b9b044bbd3e0c69b9c7	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/registry/dc	JAVASCRIPT	RegularFile, Executable	REG	/zh-CN/component/up	element.eleme.io	/		http	http://ele	19701817-13e0-441f-8512-df2fc0569de0
31	.js	main.2485230bcb7306882473.j	ASCII text, with very long lines, with no line terminato	/sample_C1.zip/NVMe/docker/ov	JAVASCRIPT	RegularFile, Executable	REG	!#change-propagation	angular.io	/docs/ts/latest/api/common/index/NgFor-directive.html		https	https://angular.io/docs/ts/latest/api/common/index/NgFor-di	
32	.txt	3rdpartylicenses.txt	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/docker/ov	TEXT_FILE	RegularFile, Text, Non	REG		kossnocorp.mit-license.org			http	http://kossnocorp.mit-license.org	
33	.txt	3rdpartylicenses.txt	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/registry/dc	TEXT_FILE	RegularFile, Text, Non	REG		kossnocorp.mit-license.org			http	http://kos	19701817-13e0-441f-8512-df2fc0569de0
34	.txt	3rdpartylicenses.txt	UTF-8 Unicode text, with very long lines	/sample_C1.zip/NVMe/registry/dc	TEXT_FILE	RegularFile, Text, Non	REG		tldrlegal.com	/license/mit-license		https	https://tld	19701817-13e0-441f-8512-df2fc0569de0
35		webmnt	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/registry/dc	ELF	RegularFile, Executable	REG		beego.me	/docs/module/toolbox.md">Toolbox</a		http	http://bee	19701817-13e0-441f-8512-df2fc0569de0
36		webmnt	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		beego.me	/docs/advantage/monitor.md">Live		http	http://bee	19701817-13e0-441f-8512-df2fc0569de0
37	.conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/registry/dc	CONFIG	RegularFile, Configurat	REG		redis.io	/topics/client-side-caching		https	https://re	19701817-13e0-441f-8512-df2fc0569de0
38	.conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/docker/ov	CONFIG	RegularFile, Configurat	REG		redis.io	/topics/acl		https	https://redis.io/topics/acl	
39	.conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/docker/ov	CONFIG	RegularFile, Configurat	REG		redis.io	/topics/persistence		http	http://redis.io/topics/persistence	
40	.conf	redis.conf	ASCII text	/sample_C1.zip/NVMe/registry/dc	CONFIG	RegularFile, Configurat	REG		antirez.com	/post/redis-persistence-demystified.html		http	http://ant	19701817-13e0-441f-8512-df2fc0569de0
41	.html	demo_index.html	HTML document text	/sample_C1.zip/NVMe/docker/ov	HTML	RegularFile, Document	REG		img.alicdn.com	/tps/i4/TB1_oz6GVXXXXaFXpXXUDFnIXXX-64-64.ico		https	https://img.alicdn.com/tps/i4/TB1_oz6GVXXXXaFXpXXUDFnIXX	
42	.h	bn.h	C source text C source text C source text	/sample_C1.zip/NVMe/docker/ov	C_SOURCE	RegularFile, Sourcecod	REG		magma.maths.usyd.edu.a	/calc		http	http://magma.maths.usyd.edu.au/calc	
43	.h	bn.h	C source text C source text C source text	/sample_C1.zip/NVMe/registry/dc	C_SOURCE	RegularFile, Sourcecod	REG		magma.maths.usyd.edu.a	/calc		http	http://ma	19701817-13e0-441f-8512-df2fc0569de0
44		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		curl.haxx.se	/libcurl/c/curl_easy_setopt.html		https	https://curl.haxx.se/libcurl/c/curl_easy_setopt.html	
45		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/registry/dc	ELF	RegularFile, Executable	REG		curl.haxx.se	/libcurl/c/curl_easy_setopt.html		https	https://cu	19701817-13e0-441f-8512-df2fc0569de0
46		curl	ELF 64-bit LSB executable, x86-64, version 1 (SYSV) (Lec	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		curl.haxx.se	/docs/sslcerts.html		https	https://curl.haxx.se/docs/sslcerts.html	
47		webmt	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		schemas.openxmlformat	/officeDocument/2006/relationships		http	http://schemas.openxmlformats.org/officeDocument/2006/rel	
48		webmt	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linu	/sample_C1.zip/NVMe/docker/ov	ELF	RegularFile, Executable	REG		schemas.openxmlformat	drawingml/2006/spreadsheetDrawing		http	http://schemas.openxmlformats.org/drawingml/2006/spreadsl	

c1_url-strings +

Figure 44: C1 Infoleak URL report (Jarvis)

Sample C1 Finite State Platform Scan Report Excerpts

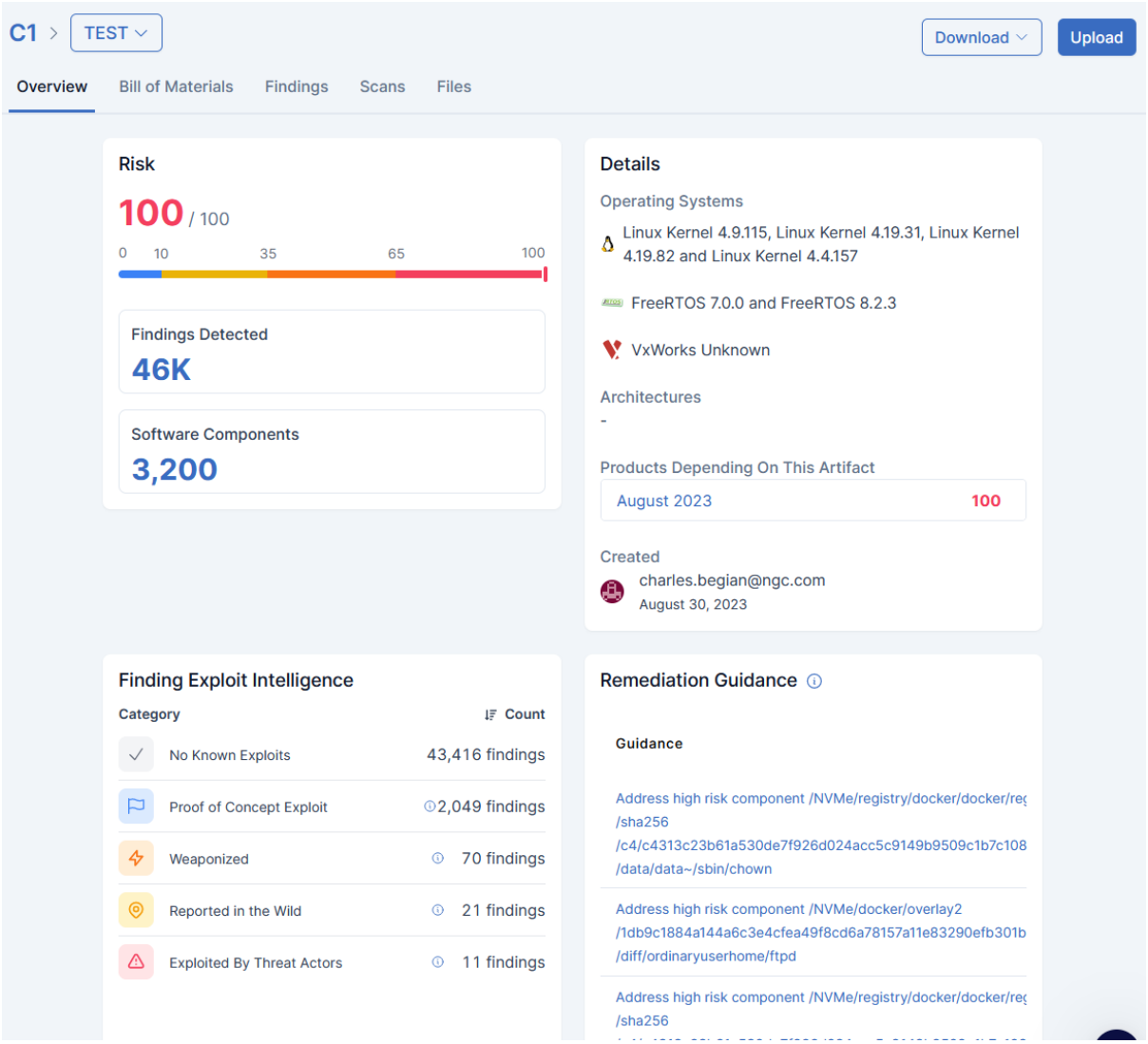


Figure 45; C1 Scan Overview (Finite State Platform)

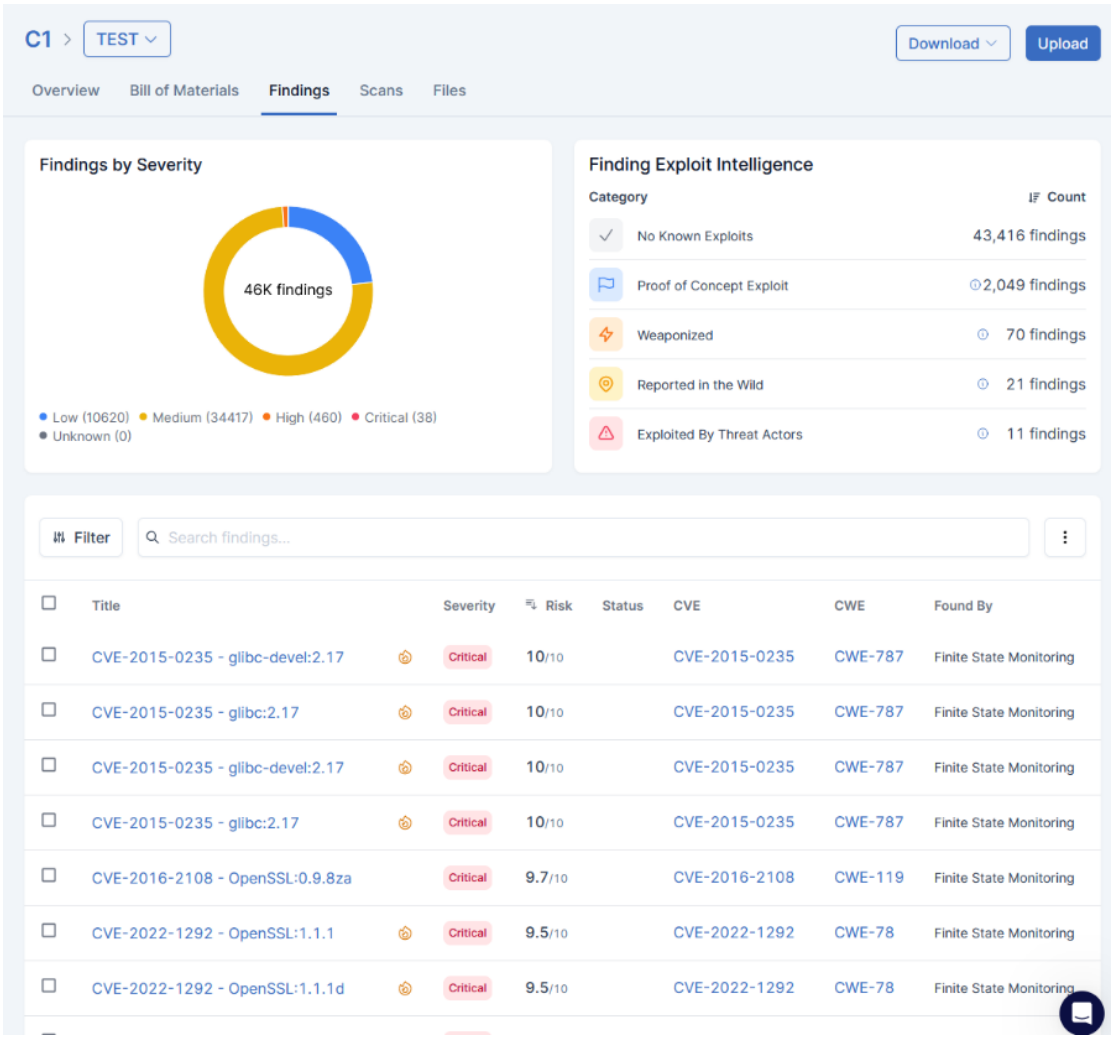


Figure 46: C1 Scan Findings (Finite State Platform)

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)

A	B	C	D	G	H	I
vulnIdFromTool	riskScore	cvssV3Sco	cvssVectorString	affectedComponents	exploitCount	maxExploitMaturity
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	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-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-2016-7054	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-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
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	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	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-2014-9761	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	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
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	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:4.19.31	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	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:4.19.31	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:1.1.1k	1	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:2.2.6	1	poc

C1_TEST.exploit-intel

Figure 48: C1 CVE Exploitability (Finite State Platform)

APPENDIX D: CST SCAN REPORT EXCERPTS FOR SAMPLE C2

Sample C2 Black Duck Scan Report Excerpts

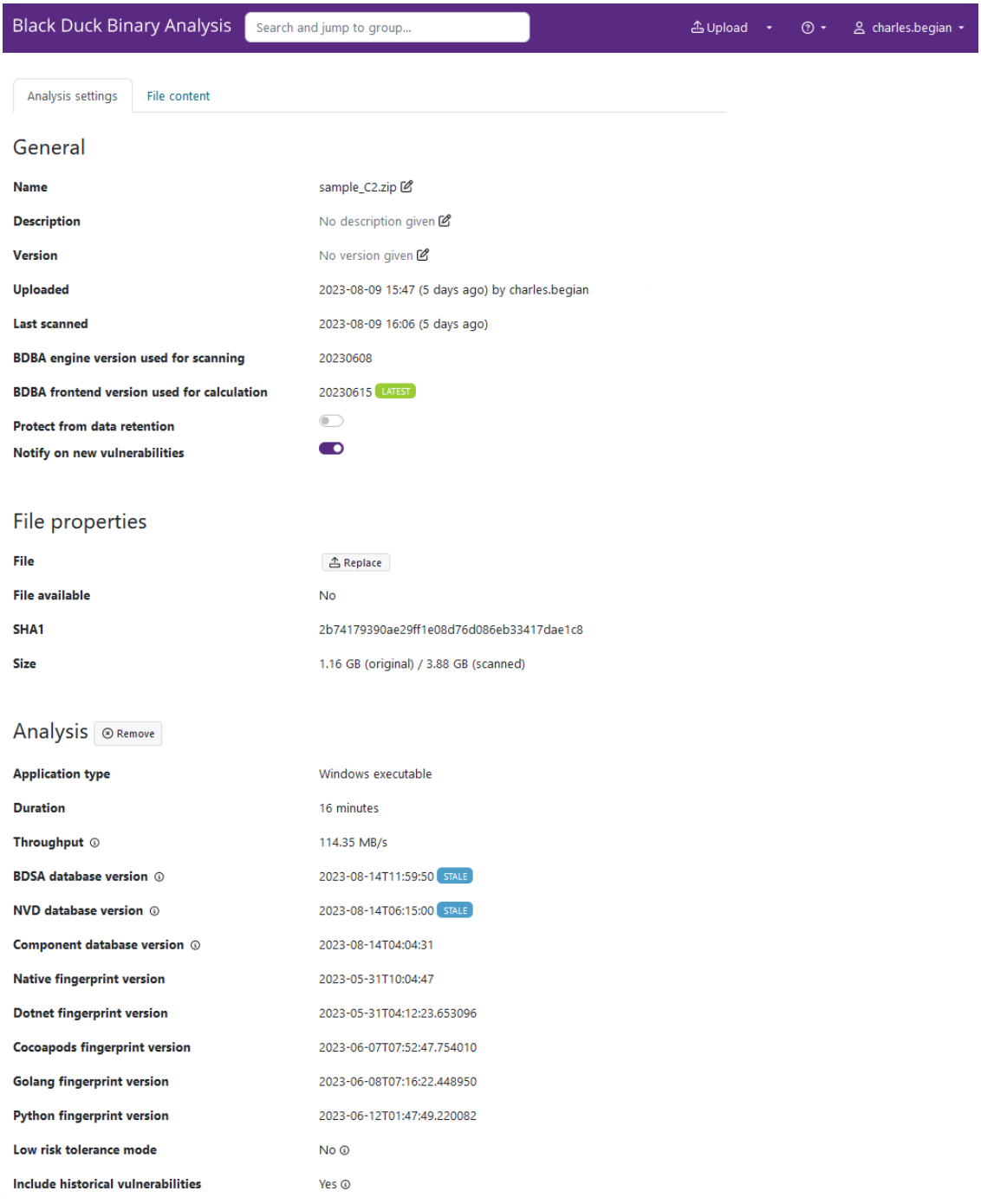
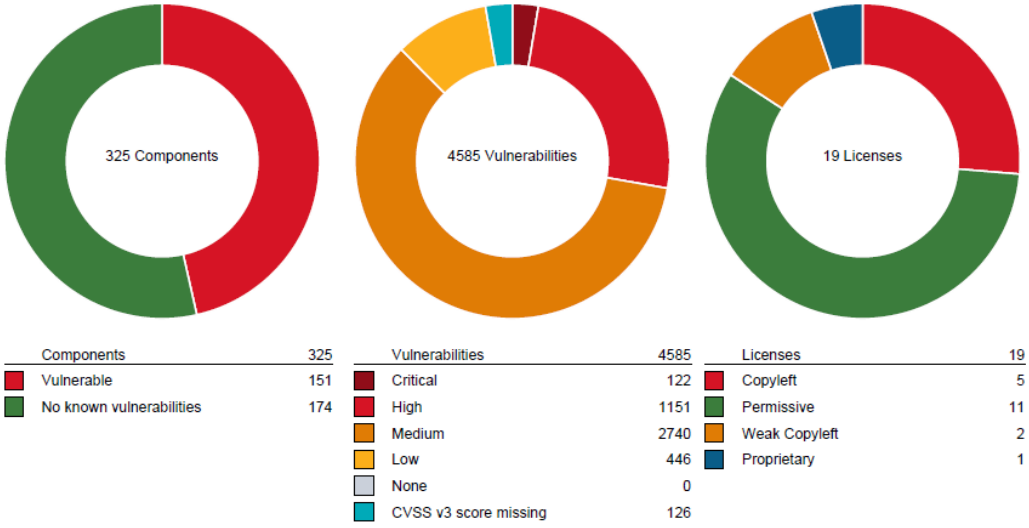


Figure 49: C2 Scan Overview (Black Duck)

Report generated 2023-08-13T22:48:18Z
https://protecode-sc.com/products/24697604

sample_C2.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY



Components	325
Vulnerable	151
No known vulnerabilities	174

Vulnerabilities	4585
Critical	122
High	1151
Medium	2740
Low	446
None	0
CVSS v3 score missing	126

Licenses	19
Copyleft	5
Permissive	11
Weak Copyleft	2
Proprietary	1

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

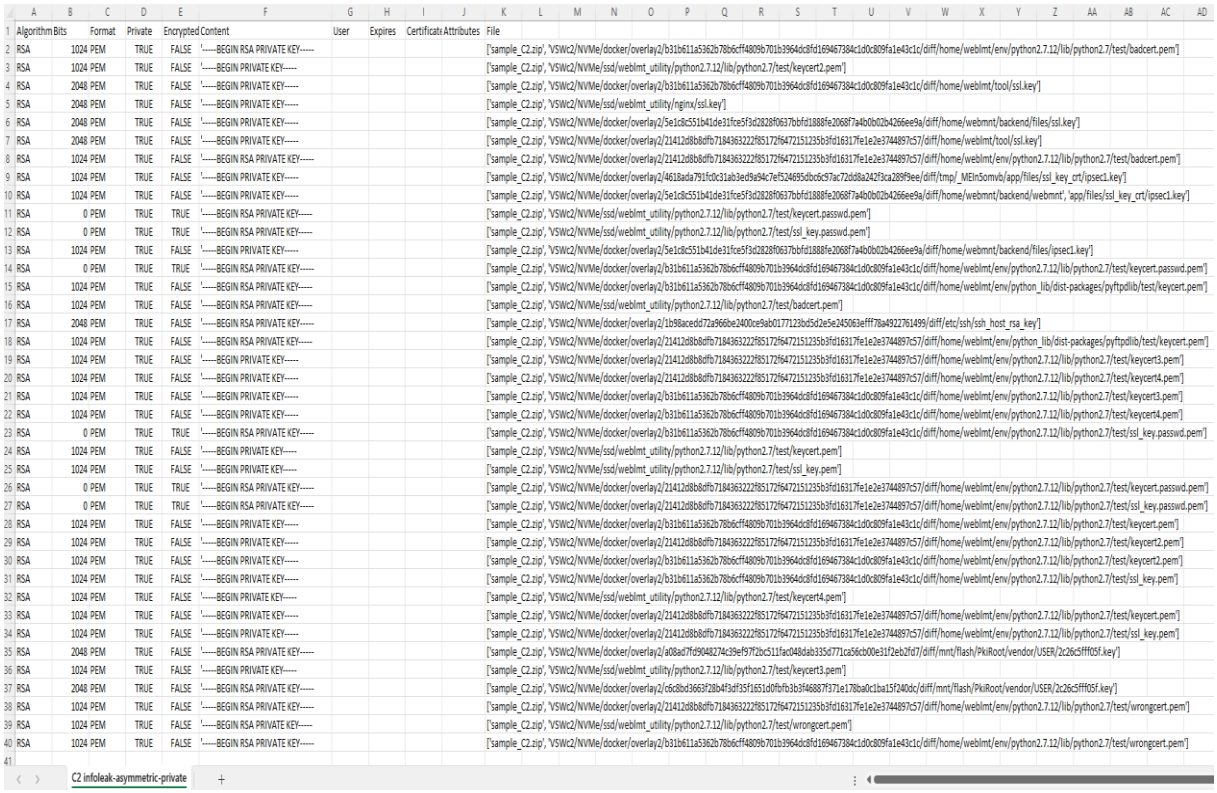
Details

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

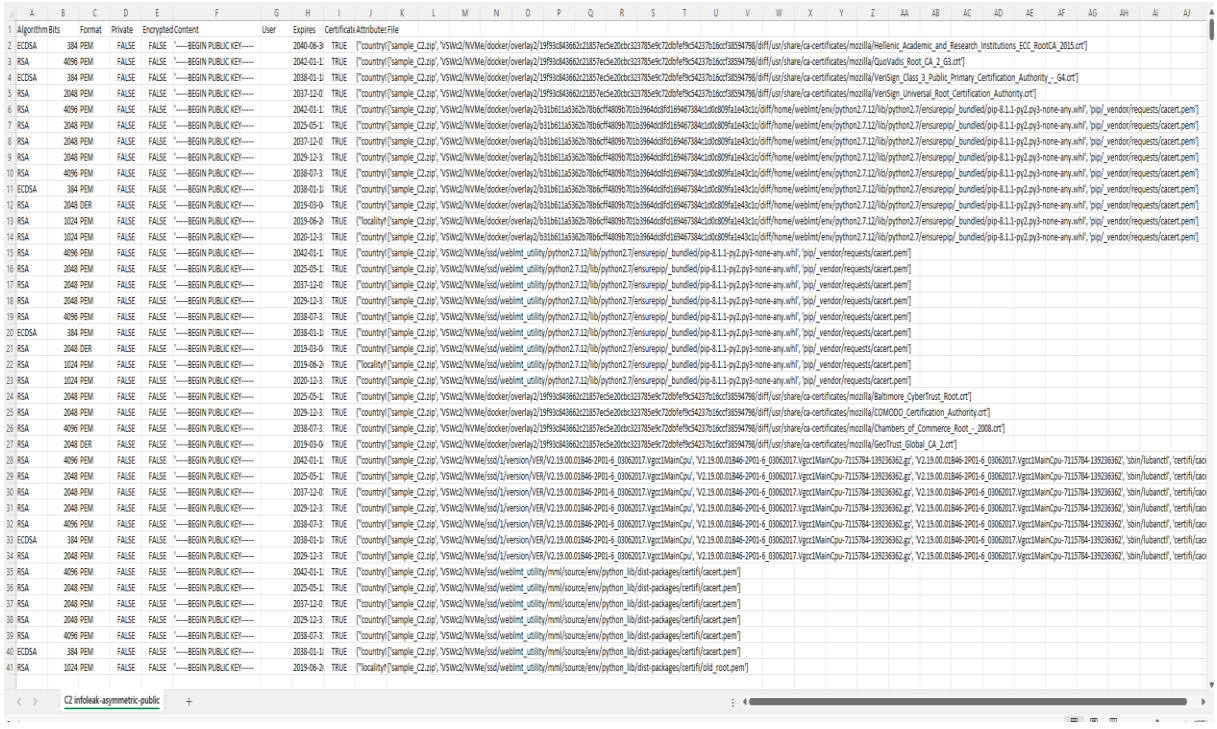
Figure 51: C2 Information leaks (Black Duck)



Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/badcert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/keycert2.pem']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/tool/ssl.key']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/nginx/ssl.key']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/5e1c8c551b41de31fce5f3d2828f0637bbfd1888fe2068f7a4b0b02b4266ee9a/diff/home/webmnt/backend/files/ssl.key']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/tool/ssl.key']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/badcert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4618ada791fc0c31ab3ed9a94c7ef524695dbc6c97ac72dd8a242f3ca289f9ee/diff/tmp/_MEIn5omvb/app/files/ssl_key_crt/ipsec1.key']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/5e1c8c551b41de31fce5f3d2828f0637bbfd1888fe2068f7a4b0b02b4266ee9a/diff/home/webmnt/backend/webmnt', 'app/files/ssl_key_crt/ipsec1.key']
RSA	0	PEM	TRUE	TRUE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/keycert.passwd.pem']
RSA	0	PEM	TRUE	TRUE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/ssl_key.passwd.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/5e1c8c551b41de31fce5f3d2828f0637bbfd1888fe2068f7a4b0b02b4266ee9a/diff/home/webmnt/backend/files/ipsec1.key']
RSA	0	PEM	TRUE	TRUE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert.passwd.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python_lib/dist-packages/pyftpdlib/test/keycert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/badcert.pem']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/1b98aced072a966be2400ce9ab0177123bd5d2e5e245063efff78a492276149 9/diff/etc/ssh/ssh_host_rsa_key']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python_lib/dist-packages/pyftpdlib/test/keycert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert3.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert4.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert3.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert4.pem']
RSA	0	PEM	TRUE	TRUE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/ssl_key.passwd.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/keycert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/ssl_key.pem']
RSA	0	PEM	TRUE	TRUE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert.passwd.pem']
RSA	0	PEM	TRUE	TRUE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/ssl_key.passwd.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert2.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert2.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/ssl_key.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/keycert4.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/keycert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/ssl_key.pem']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/a08ad7fd9048274c39ef97f2bc511fac048dab335d771ca56cb00e31f2eb2fd7/diff/mnt/flash/PkiRoot/vendor/USER/2c26c5fff05f.key']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/keycert3.pem']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c6c8bd3663f28b4f3df35f1651d0fbfb3bf46887f371e178ba0c1ba15f240dc/diff/mnt/flash/PkiRoot/vendor/USER/2c26c5fff05f.key']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/wrongcert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/test/wrongcert.pem']
RSA	1024	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/test/wrongcert.pem']

C2 infoleak-asymmetric-private

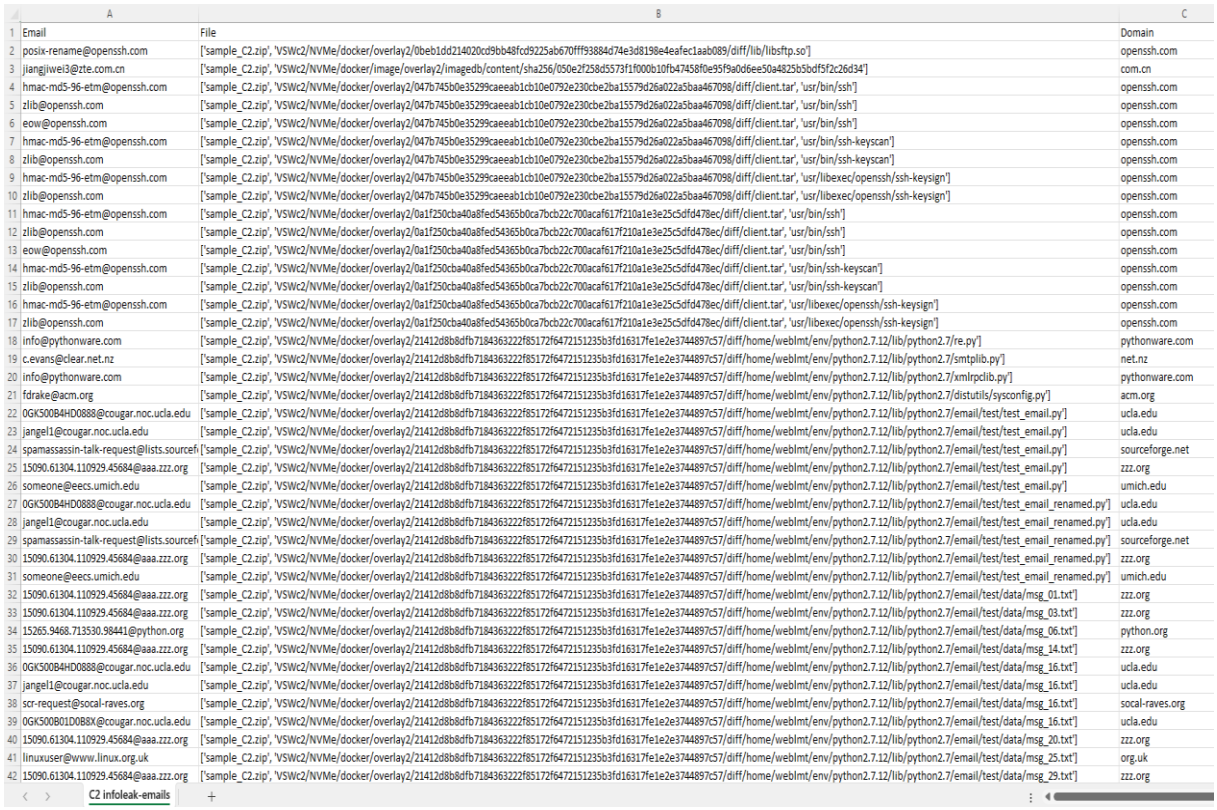
Figure 52: C2 Asymmetric keys (Black Duck)



Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File
ECDSA	384	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2040-06-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2042-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/QuoVadis_Root_CA_2_G3.crt']
ECDSA	384	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4.crt']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2037-12-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/VeriSign_Universal_Root_Certification_Authority.crt']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2042-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2025-05-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2037-12-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-07-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
ECDSA	384	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	DER	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2019-03-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	1024	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2019-06-2	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	1024	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2020-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/b31b611a5362b78b6cff4809b701b3964dc8fd169467384c1d0c809fa1e43c1c/diff/home/weblmt/env/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2042-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2025-05-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2037-12-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-07-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
ECDSA	384	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	DER	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2019-03-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	1024	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2019-06-2	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	1024	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2020-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/python2.7.12/lib/python2.7/ensurepip/_bundled/pip-8.1.1-py2.py3-none-any.whl', 'pip/_vendor/requests/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2025-05-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/Baltimore_CyberTrust_Root.crt']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/COMODO_Certification_Authority.crt']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-07-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/Chambers_of_Commerce_Root_-_2008.crt']
RSA	2048	DER	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2019-03-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857e5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/share/ca-certificates/mozilla/GeoTrust_Global_CA_2.crt']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2042-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2025-05-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2037-12-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-07-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
ECDSA	384	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu/', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362.gz', 'V2.19.00.01846-2P01-6_03062017.Vgrc1MainCpu-7115784-139236362', 'sbin/lubanctl', 'certifi/cacert
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2042-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2025-05-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2037-12-0	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/cacert.pem']
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-07-3	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/cacert.pem']
ECDSA	384	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2038-01-1	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/cacert.pem']
RSA	1024	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2019-06-2	TRUE		['country\['sample_C2.zip', 'VSWc2/NVMe/ssd/weblmt_utility/mml/source/env/python_lib/dist-packages/certifi/old_root.pem']

C2 infoleak-asymmetric-public

Figure 53: C2 Symmetric keys (Black Duck)



	A	B	C
1	Email	File	Domain
2	posix-rename@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0beb1dd214020cd9bb48fcd9225ab670fff93884d74e3d8198e4eafec1aab089/diff/lib/libsftp.so']	openssh.com
3	jiangjiwei3@zte.com.cn	['sample_C2.zip', 'VSWc2/NVMe/docker/image/overlay2/imagedb/content/sha256/050e2f258d5573f1f000b10fb47458f0e95f9a0d6ee50a4825b5bdf5f2c26d34']	com.cn
4	hmac-md5-96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh']	openssh.com
5	zlib@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh']	openssh.com
6	eow@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh']	openssh.com
7	hmac-md5-96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
8	zlib@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
9	hmac-md5-96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
10	zlib@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/047b745b0e35299caeeab1cb10e0792e230cbe2ba15579d26a022a5baa467098/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
11	hmac-md5-96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh']	openssh.com
12	zlib@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh']	openssh.com
13	eow@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh']	openssh.com
14	hmac-md5-96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
15	zlib@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/bin/ssh-keyscan']	openssh.com
16	hmac-md5-96-etm@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
17	zlib@openssh.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/0a1f250cba40a8fed54365b0ca7bcb22c700acaf617f210a1e3e25c5dfd478ec/diff/client.tar', 'usr/libexec/openssh/ssh-keysign']	openssh.com
18	info@pythonware.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/re.py']	pythonware.com
19	c.evans@clear.net.nz	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/smtplib.py']	net.nz
20	info@pythonware.com	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/xmlrpclib.py']	pythonware.com
21	fdrake@acm.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/distutils/sysconfig.py']	acm.org
22	0GK500B4HD0888@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
23	jangel1@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
24	spamassassin-talk-request@lists.sourcefi	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email.py']	sourceforge.net
25	15090.61304.110929.45684@aaa.zzz.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email.py']	zzz.org
26	someone@eecs.umich.edu	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email.py']	umich.edu
27	0GK500B4HD0888@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_renamed.py']	ucla.edu
28	jangel1@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_renamed.py']	ucla.edu
29	spamassassin-talk-request@lists.sourcefi	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email_renamed.py']	sourceforge.net
30	15090.61304.110929.45684@aaa.zzz.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email_renamed.py']	zzz.org
31	someone@eecs.umich.edu	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/test_email_renamed.py']	umich.edu
32	15090.61304.110929.45684@aaa.zzz.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_01.txt']	zzz.org
33	15090.61304.110929.45684@aaa.zzz.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_03.txt']	zzz.org
34	15265.9468.713530.98441@python.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_06.txt']	python.org
35	15090.61304.110929.45684@aaa.zzz.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_14.txt']	zzz.org
36	0GK500B4HD0888@cougar.noc.ucla.edu	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_16.txt']	ucla.edu
37	jangel1@cougar.noc.ucla.edu	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_16.txt']	ucla.edu
38	scr-request@socal-raves.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_16.txt']	socal-raves.org
39	0GK500B01D0B8X@cougar.noc.ucla.edu	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_16.txt']	ucla.edu
40	15090.61304.110929.45684@aaa.zzz.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_20.txt']	zzz.org
41	linuxuser@www.linux.org.uk	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python2.7.12/lib/python2.7/email/test/data/msg_25.txt']	org.uk
42	15090.61304.110929.45684@aaa.zzz.org	['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

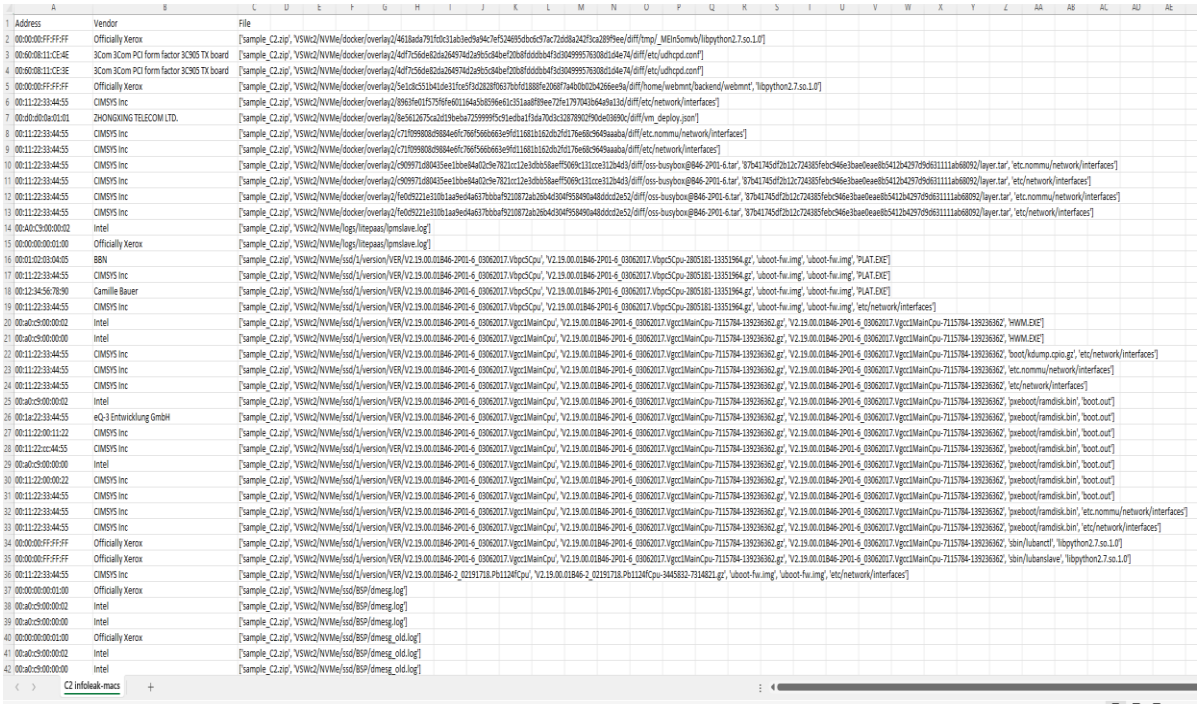
C2 infoleak-emails

Figure 54: C2 Infoleak email addresses (Black Duck)

	A	B	C	D	E	F	G	H	I	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']									
6	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']									
8	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']									
10	173.1.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
11	173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
12	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
13	192.254.1.18	FALSE	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']									
14	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01a674e05ae1905d949cbd6e1ef87343e9b89ada46dbef41afd69ea987c16d71/config.v2.json']									
15	192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01a674e05ae1905d949cbd6e1ef87343e9b89ada46dbef41afd69ea987c16d71/config.v2.json']									
16	173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01a674e05ae1905d949cbd6e1ef87343e9b89ada46dbef41afd69ea987c16d71/config.v2.json']									
17	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01a674e05ae1905d949cbd6e1ef87343e9b89ada46dbef41afd69ea987c16d71/config.v2.json']									
18	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01e6cd8f54d99067f2bb3a011f3bb05ad9d79db98c377024fe81862c3351da7b/config.v2.json']									
19	192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01e6cd8f54d99067f2bb3a011f3bb05ad9d79db98c377024fe81862c3351da7b/config.v2.json']									
20	173.1.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01e6cd8f54d99067f2bb3a011f3bb05ad9d79db98c377024fe81862c3351da7b/config.v2.json']									
21	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01e6cd8f54d99067f2bb3a011f3bb05ad9d79db98c377024fe81862c3351da7b/config.v2.json']									
22	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01f661293742bb28efab029b6d4a220bef338df4e70c5e5dc08302f4060e0558/config.v2.json']									
23	192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01f661293742bb28efab029b6d4a220bef338df4e70c5e5dc08302f4060e0558/config.v2.json']									
24	173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01f661293742bb28efab029b6d4a220bef338df4e70c5e5dc08302f4060e0558/config.v2.json']									
25	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/01f661293742bb28efab029b6d4a220bef338df4e70c5e5dc08302f4060e0558/config.v2.json']									
26	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/02fde1b64f4990366ac3eb11ac0e7f50e1b44846acaec81a7a9f250b66bf0e47/config.v2.json']									
27	192.254.128.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/02fde1b64f4990366ac3eb11ac0e7f50e1b44846acaec81a7a9f250b66bf0e47/config.v2.json']									
28	173.254.128.2	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/02fde1b64f4990366ac3eb11ac0e7f50e1b44846acaec81a7a9f250b66bf0e47/config.v2.json']									
29	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/02fde1b64f4990366ac3eb11ac0e7f50e1b44846acaec81a7a9f250b66bf0e47/config.v2.json']									
30	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/07824cdfd829065f53ad1bd8acb3633c2dfb5ac3f6887a03252c3cebda9b4d57/config.v2.json']									
31	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/07824cdfd829065f53ad1bd8acb3633c2dfb5ac3f6887a03252c3cebda9b4d57/config.v2.json']									
32	127.0.0.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/07824cdfd829065f53ad1bd8acb3633c2dfb5ac3f6887a03252c3cebda9b4d57/hosts']									
33	8.8.8.8	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/07824cdfd829065f53ad1bd8acb3633c2dfb5ac3f6887a03252c3cebda9b4d57/resolv.conf']									
34	8.8.4.4	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/07824cdfd829065f53ad1bd8acb3633c2dfb5ac3f6887a03252c3cebda9b4d57/resolv.conf']									
35	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0880e826c205d9417dc8954bcb785f3799e049719441ac52631a808109a7020e/config.v2.json']									
36	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0880e826c205d9417dc8954bcb785f3799e049719441ac52631a808109a7020e/config.v2.json']									
37	127.0.0.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0880e826c205d9417dc8954bcb785f3799e049719441ac52631a808109a7020e/hosts']									
38	8.8.8.8	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0880e826c205d9417dc8954bcb785f3799e049719441ac52631a808109a7020e/resolv.conf']									
39	8.8.4.4	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0880e826c205d9417dc8954bcb785f3799e049719441ac52631a808109a7020e/resolv.conf']									
40	192.254.1.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0f7ddf6d18a3e31e90e7a9f8c1ce3a558da9d4b440dc3c1adcb6e212fcb8d21d/config.v2.json']									
41	173.254.95.16	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0f7ddf6d18a3e31e90e7a9f8c1ce3a558da9d4b440dc3c1adcb6e212fcb8d21d/config.v2.json']									
42	127.0.0.1	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/containers/0f7ddf6d18a3e31e90e7a9f8c1ce3a558da9d4b440dc3c1adcb6e212fcb8d21d/hosts']									

C2 infoleak-ips

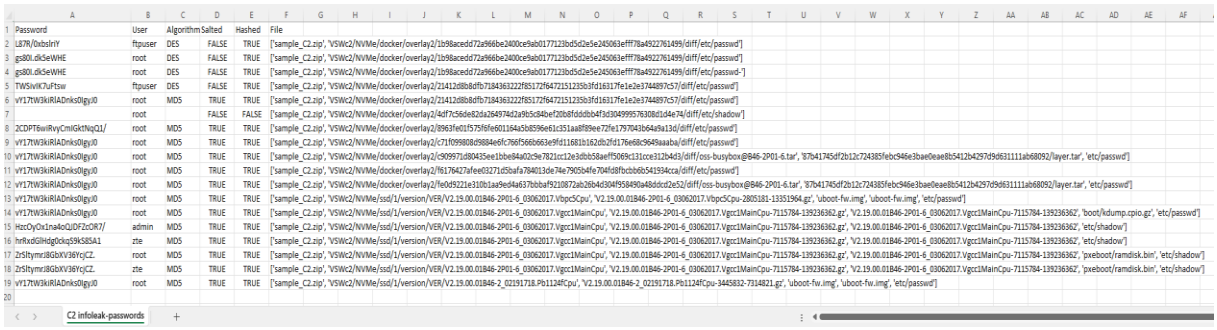
Figure 55: C2 Infoleak IP addresses (Black Duck)



	A	B	C
1	Address	Vendor	File
2	00:00:00:FF:FF:FF	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4618ada791cf0c31ab3ed9a94c7ef524695dbc6d7ac72dd8a242f3ca289f9ee/diff/tmp/_MEIn5omvb/libpython2.7.so.1.0']
3	00:60:08:11:CE:4E	3Com 3Com PCI form factor 3C905 TX board	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df75c6de82da264974d2a9b5c840bef20b8fdddbb4f3d30499957630 8d1d4e74/diff/etc/udhcpd.conf']
4	00:60:08:11:CE:3E	3Com 3Com PCI form factor 3C905 TX board	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df75c6de82da264974d2a9b5c840bef20b8fdddbb4f3d30499957630 8d1d4e74/diff/etc/udhcpd.conf']
5	00:00:00:FF:FF:FF	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/5e1c8c551b41de31fce5f3d28287f0637bbfd1888fe2068f7a4b0b02b4266ee9a/diff/home/webmnt/backend/webmnt', 'libpython2.7.so.1.0']
6	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/8963fe01f575f6fe601164a5b8596e61c351aa8f89ee72fe17970430b64a9a13d/diff/etc/network/interfaces']
7	00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/8e5612675ca2d19beba72599995fc91edba1f3da70d3c32878902f90de03690c/diff/vm_deploy.json']
8	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c71f099808d9884e6fc766f566b663e9fd11681b162db2fd176e68c9649aaaba/diff/etc.nommu/network/interfaces']
9	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c71f099808d9884e6fc766f566b663e9fd11681b162db2fd176e68c9649aaaba/diff/etc/network/interfaces']
10	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c909971c680435ee1bbe84a02c9e7821cc12e3dbb58aeff5069c131cce312b4d3/diff/oss-busybox@846-2P01-6.tar', '87b41745df2b12c724385febc946e3bae0eae8b5412b4297d9d631111ab68092/layer.tar', 'etc.nommu/network/interfaces']
11	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c909971c680435ee1bbe84a02c9e7821cc12e3dbb58aeff5069c131cce312b4d3/diff/oss-busybox@846-2P01-6.tar', '87b41745df2b12c724385febc946e3bae0eae8b5412b4297d9d631111ab68092/layer.tar', 'etc/network/interfaces']
12	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/fe0d5221e310b1aa9ed4a637bbbaf9210872ab26b4d304f958490a48ddcd2e52/diff/oss-busybox@846-2P01-6.tar', '87b41745df2b12c724385febc946e3bae0eae8b5412b4297d9d631111ab68092/layer.tar', 'etc.nommu/network/interfaces']
13	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/fe0d5221e310b1aa9ed4a637bbbaf9210872ab26b4d304f958490a48ddcd2e52/diff/oss-busybox@846-2P01-6.tar', '87b41745df2b12c724385febc946e3bae0eae8b5412b4297d9d631111ab68092/layer.tar', 'etc/network/interfaces']
14	00:A0:C9:00:00:02	Intel	['sample_C2.zip', 'VSWc2/NVMe/logs/litepaas/lpmslave.log']
15	00:00:00:00:01:00	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/logs/litepaas/lpmslave.log']
16	00:01:02:03:04:05	BBN	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VbpcSCpu', 'V2.19.00.01846-2P01-6_03062017.VbpcSCpu-2805181-13351964.gz', 'uboot-fw.img', 'uboot-fw.img', 'PLAT.EXE']
17	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VbpcSCpu', 'V2.19.00.01846-2P01-6_03062017.VbpcSCpu-2805181-13351964.gz', 'uboot-fw.img', 'uboot-fw.img', 'PLAT.EXE']
18	00:12:34:56:78:90	Camille Bauer	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VbpcSCpu', 'V2.19.00.01846-2P01-6_03062017.VbpcSCpu-2805181-13351964.gz', 'uboot-fw.img', 'uboot-fw.img', 'PLAT.EXE']
19	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VbpcSCpu', 'V2.19.00.01846-2P01-6_03062017.VbpcSCpu-2805181-13351964.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/network/interfaces']
20	00:a0:c9:00:00:02	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'HWM.EXE']
21	00:a0:c9:00:00:00	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'HWM.EXE']
22	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'boot/kdump.cpio.gz', 'etc/network/interfaces']
23	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'etc.nommu/network/interfaces']
24	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'etc/network/interfaces']
25	00:a0:c9:00:00:02	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
26	00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
27	00:11:22:00:11:22	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
28	00:11:22:cc:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
29	00:a0:c9:00:00:00	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
30	00:11:22:00:00:22	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
31	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'boot.out']
32	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'etc.nommu/network/interfaces']
33	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'etc/network/interfaces']
34	00:00:00:FF:FF:FF	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'sbin/lubanctl', 'libpython2.7.so.1.0']
35	00:00:00:FF:FF:FF	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'sbin/lubanslave', 'libpython2.7.so.1.0']
36	00:11:22:33:44:55	CIMSYS Inc	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01B46-2_02191718.Pb1124fCpu', 'V2.19.00.01B46-2_02191718.Pb1124fCpu-3445832-7314821.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/network/interfaces']
37	00:00:00:00:01:00	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/ssd/BSP/dmesg.log']
38	00:a0:c9:00:00:02	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/BSP/dmesg.log']
39	00:a0:c9:00:00:00	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/BSP/dmesg.log']
40	00:00:00:00:01:00	Officially Xerox	['sample_C2.zip', 'VSWc2/NVMe/ssd/BSP/dmesg_old.log']
41	00:a0:c9:00:00:02	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/BSP/dmesg_old.log']
42	00:a0:c9:00:00:00	Intel	['sample_C2.zip', 'VSWc2/NVMe/ssd/BSP/dmesg_old.log']

C2 infoleak-macs

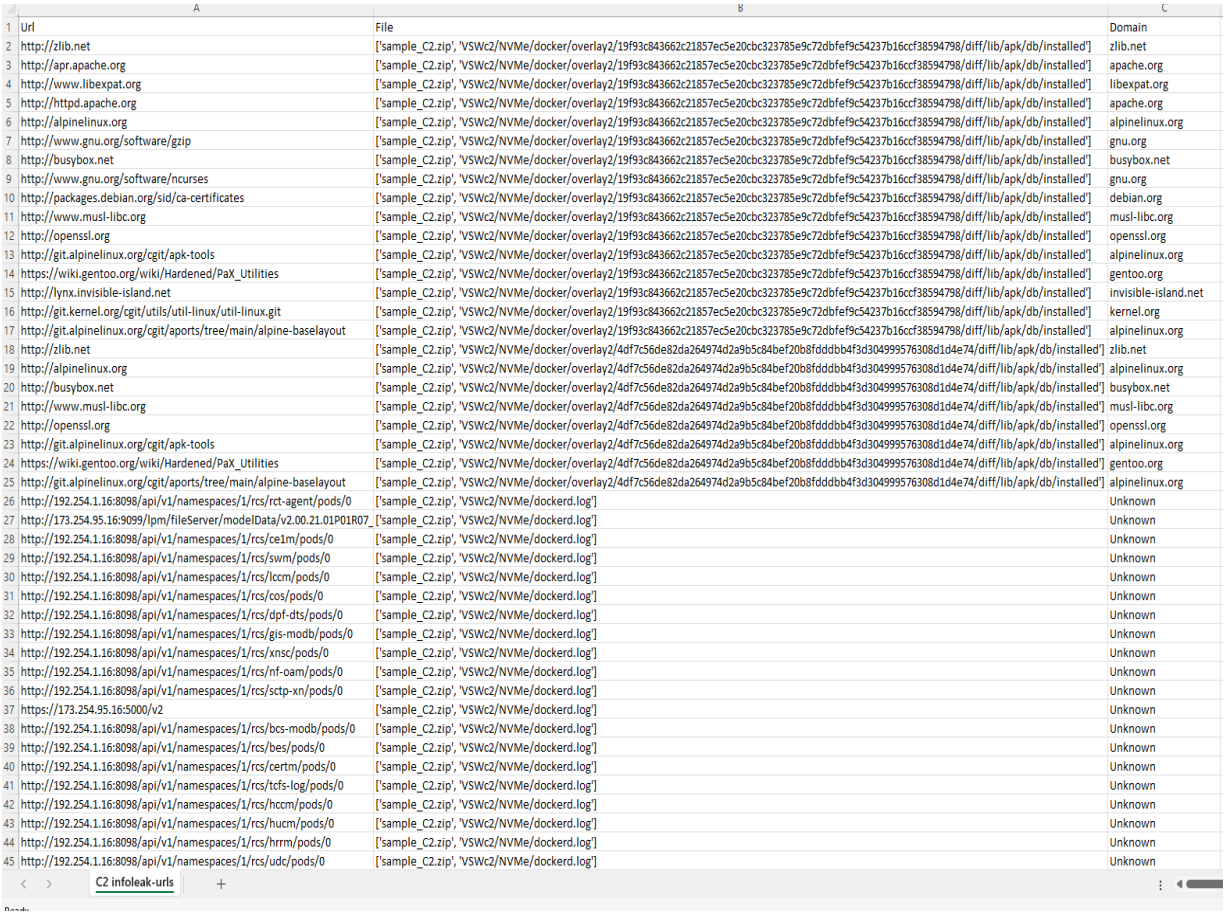
Figure 56: C2 Infoleak MAC addresses (Black Duck)



	A	B	C	D	E	F
1	Password	User	Algorithm	Salted	Hashed	File
2	L87R/0xbsnlY	ftpuser	DES	FALSE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/1b98acedd72a966be2400ce9ab0177123bd5d2e5e245063efff78a4922761499/diff/etc/passwd']
3	gs80l.dk5eWHE	root	DES	FALSE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/1b98acedd72a966be2400ce9ab0177123bd5d2e5e245063efff78a4922761499/diff/etc/passwd']
4	gs80l.dk5eWHE	root	DES	FALSE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/1b98acedd72a966be2400ce9ab0177123bd5d2e5e245063efff78a4922761499/diff/etc/passwd-']
5	TWSiiVIK7uFtsw	ftpuser	DES	FALSE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f647215123 5b3fd16317fe1e2e3744897c57/diff/etc/passwd']
6	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/21412d8b8dfb7184363222f85172f647215123 5b3fd16317fe1e2e3744897c57/diff/etc/passwd']
7		root		FALSE	FALSE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c840bef20b8fdddbb4f3d30499957630 8d1d4e74/diff/etc/shadow']
8	2CDPT8wiRvyCmIGktNqQ1/	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/8963fe01f575f6fe601164a5b8596e61c351aa8f89ee72fe17970430b64a9a13d/diff/etc/passwd']
9	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c71f099808d9884e6fc766f566b663e9fd11681b162db2fd176e68c9649aaaba/diff/etc/passwd']
10	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/c909971d80435ee1bbe84a02c9e7821cc12e3dbb58aeff5069c131cce312b4d3/diff/oss-busybox@846-2P01-6.tar', '87b41745df2b12c724385febc946e3bae0eae8b5412b4297d9d631111ab68092/layer.tar', 'etc/passwd']
11	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/f617642 7afee03271d5bafa784013de74e7905b4fe704fd8fbcbb6b541934cca/diff/etc/passwd']
12	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/fe0d5221e310b1aa9ed4a637bbbaf9210872ab26b4d304f958490a48ddcd2e52/diff/oss-busybox@846-2P01-6.tar', '87b41745df2b12c724385febc946e3bae0eae8b5412b4297d9d631111ab68092/layer.tar', 'etc/passwd']
13	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VbpcSCpu', 'V2.19.00.01846-2P01-6_03062017.VbpcSCpu-2805181-13351964.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/passwd']
14	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'boot/kdump.cpio.gz', 'etc/passwd']
15	HzcOyOx1na4oQJDF2zOR7/	admin	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'etc/shadow']
16	hrRxdGIHdg0ckq59kS85A1	zte	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'etc/shadow']
17	ZrSItymziBGbXV36YcjCZ.	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'etc/shadow']
18	ZrSItymziBGbXV36YcjCZ.	zte	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01846-2P01-6_03062017.VgccMainCpu', 'V2.19.00.01846-2P01-6_03062017.VgccMainCpu-7115784-139236362.gz', 'V2.19.00.01B46-2P01-6_03062017.VgccMainCpu-7115784-139236362', 'pxeboot/ramdisk.bin', 'etc/shadow']
19	vY17tW3kiRIADnksOIguv0	root	MD5	TRUE	TRUE	['sample_C2.zip', 'VSWc2/NVMe/ssd/1/version/VER/V2.19.00.01B46-2_02191718.Pb1124fCpu', 'V2.19.00.01B46-2_02191718.Pb1124fCpu-3445832-7314821.gz', 'uboot-fw.img', 'uboot-fw.img', 'etc/passwd']
20						

C2 infoleak-passwords

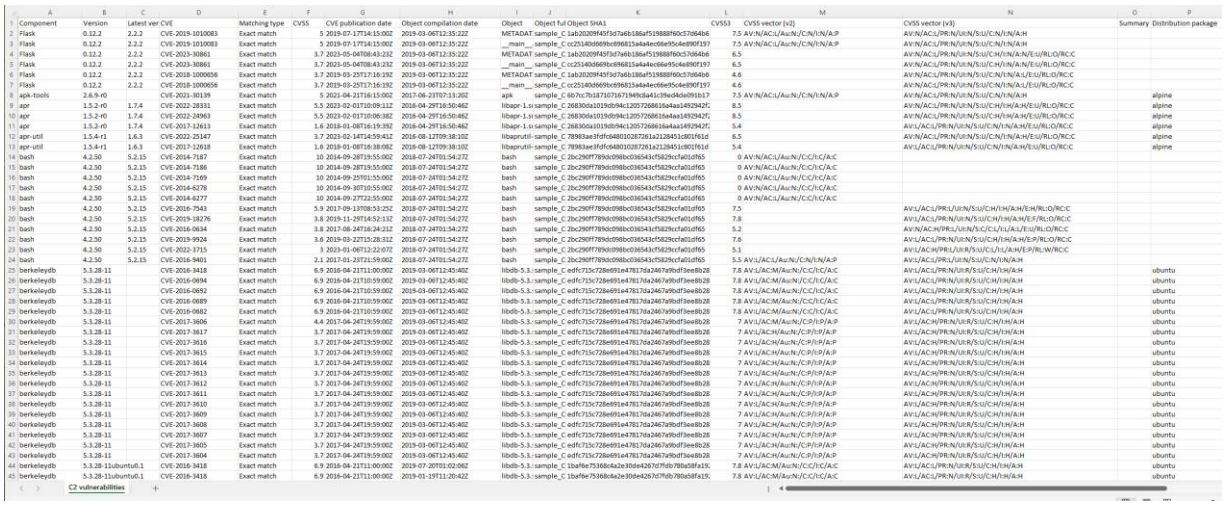
Figure 57: C2 Infoleak password (Black Duck)



	A	B	C
1	Url	File	Domain
2	http://zlib.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	zlib.net
3	http://apr.apache.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	apache.org
4	http://www.libexpat.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	libexpat.org
5	http://httpd.apache.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	apache.org
6	http://alpinelinux.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	alpinelinux.org
7	http://www.gnu.org/software/gzip	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	gnu.org
8	http://busybox.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	busybox.net
9	http://www.gnu.org/software/ncurses	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	gnu.org
10	http://packages.debian.org/sid/ca-certificates	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	debian.org
11	http://www.musl-libc.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	musl-libc.org
12	http://openssl.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	openssl.org
13	http://git.alpinelinux.org/cgit/apk-tools	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	alpinelinux.org
14	https://wiki.gentoo.org/wiki/Hardened/PaX_Utilities	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	gentoo.org
15	http://lynx.invisible-island.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/lib/apk/db/installed']	invisible-island.net
16	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
17	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
18	http://zlib.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	zlib.net
19	http://alpinelinux.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	alpinelinux.org
20	http://busybox.net	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	busybox.net
21	http://www.musl-libc.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	musl-libc.org
22	http://openssl.org	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	openssl.org
23	http://git.alpinelinux.org/cgit/apk-tools	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	alpinelinux.org
24	https://wiki.gentoo.org/wiki/Hardened/PaX_Utilities	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	gentoo.org
25	http://git.alpinelinux.org/cgit/aports/tree/main/alpine-baselayout	['sample_C2.zip', 'VSWc2/NVMe/docker/overlay2/4df7c56de82da264974d2a9b5c84bef20b8fdddbb4f3d304999576308d1d4e74/diff/lib/apk/db/installed']	alpinelinux.org
26	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/rct-agent/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
27	http://173.254.95.16:9099/lpm/fileServer/modelData/v2.00.21.01P01R07_	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
28	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/ce1m/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
29	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/swm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
30	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/lccm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
31	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cos/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
32	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/dpf-dts/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
33	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/gis-modb/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
34	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/xnsc/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
35	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/nf-oam/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
36	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/sctp-xn/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
37	https://173.254.95.16:5000/v2	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
38	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bcs-modb/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
39	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bes/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
40	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/certm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
41	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/tcfs-log/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
42	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/hccm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
43	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/hucm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
44	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/hrrm/pods/0	['sample_C2.zip', 'VSWc2/NVMe/dockerd.log']	Unknown
45	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	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Component	Version	Latest ver	CVE	Matching type	CVSS	CVE publication date	Object compilation date	Object	Object ful	Object SHA1	CVSS3	CVSS vector (v2)	CVSS vector (v3)	Summary	Distribution package
2	Flask	0.12.2	2.2.2	CVE-2019-1010083	Exact match		5 2019-07-17T14:15:00Z	2019-03-06T12:35:22Z	METADAT	sample_C	1ab20209f45f3d7a6b186af519888f60c57064b6	7.5	AV:N/AC:L/Au:N/C:N/I:N/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
3	Flask	0.12.2	2.2.2	CVE-2019-1010083	Exact match		5 2019-07-17T14:15:00Z	2019-03-06T12:35:22Z	__main__	sample_C	cc25140d669bc696815a4a4ec66e95c4e890f197	7.5	AV:N/AC:L/Au:N/C:N/I:N/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		
4	Flask	0.12.2	2.2.2	CVE-2023-30861	Exact match		3.7 2023-05-04T08:43:23Z	2019-03-06T12:35:22Z	METADAT	sample_C	1ab20209f45f3d7a6b186af519888f60c57064b6	6.5		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C		
5	Flask	0.12.2	2.2.2	CVE-2023-30861	Exact match		3.7 2023-05-04T08:43:23Z	2019-03-06T12:35:22Z	__main__	sample_C	cc25140d669bc696815a4a4ec66e95c4e890f197	6.5		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C		
6	Flask	0.12.2	2.2.2	CVE-2018-1000656	Exact match		3.7 2019-03-25T17:16:19Z	2019-03-06T12:35:22Z	METADAT	sample_C	1ab20209f45f3d7a6b186af519888f60c57064b6	4.6		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:C		
7	Flask	0.12.2	2.2.2	CVE-2018-1000656	Exact match		3.7 2019-03-25T17:16:19Z	2019-03-06T12:35:22Z	__main__	sample_C	cc25140d669bc696815a4a4ec66e95c4e890f197	4.6		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:U/RL:O/RC:C		
8	apk-tools	2.6.9-r0		CVE-2021-30139	Exact match		5 2021-04-21T16:15:00Z	2017-06-23T07:13:20Z	apk	sample_C	6b7cc7b187107167194fcda41c39ec4dea091b17	7.5	AV:N/AC:L/Au:N/C:P/I:N/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		alpine
9	apr	1.5.2-r0	1.7.4	CVE-2022-28331	Exact match		5.5 2023-02-01T10:09:11Z	2016-04-29T16:50:46Z	libapr-1.s	sample_C	26830da1019db94c12057268616a4aa1492942f2	8.5		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C		alpine
10	apr	1.5.2-r0	1.7.4	CVE-2022-24963	Exact match		5.5 2023-02-01T10:06:38Z	2016-04-29T16:50:46Z	libapr-1.s	sample_C	26830da1019db94c12057268616a4aa1492942f2	8.5		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C		alpine
11	apr	1.5.2-r0	1.7.4	CVE-2017-12613	Exact match		1.6 2018-01-08T16:19:39Z	2016-04-29T16:50:46Z	libapr-1.s	sample_C	26830da1019db94c12057268616a4aa1492942f2	5.4		AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C		alpine
12	apr-util	1.5.4-r1	1.6.3	CVE-2022-25147	Exact match		3.7 2023-02-14T14:59:41Z	2016-08-12T09:38:10Z	libaprutil	sample_C	78983ae3fdfc6480102872614212845 1c801f61d	6.5		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C		alpine
13	apr-util	1.5.4-r1	1.6.3	CVE-2017-12618	Exact match		1.6 2018-01-08T16:38:08Z	2016-08-12T09:38:10Z	libaprutil-	sample_C	78983ae3fdfc6480102872614212845 1c801f61d	5.4		AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:U/RL:O/RC:C		alpine
14	bash	4.2.50	5.2.15	CVE-2014-7187	Exact match		10 2014-09-28T19:55:00Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	0	AV:N/AC:L/Au:N/C:C/I:C/A:C			
15	bash	4.2.50	5.2.15	CVE-2014-7186	Exact match		10 2014-09-28T19:55:00Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	0	AV:N/AC:L/Au:N/C:C/I:C/A:C			
16	bash	4.2.50	5.2.15	CVE-2014-7169	Exact match		10 2014-09-25T01:55:00Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	0	AV:N/AC:L/Au:N/C:C/I:C/A:C			
17	bash	4.2.50	5.2.15	CVE-2014-6278	Exact match		10 2014-09-30T10:55:00Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	0	AV:N/AC:L/Au:N/C:C/I:C/A:C			
18	bash	4.2.50	5.2.15	CVE-2014-6277	Exact match		10 2014-09-27T22:55:00Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	0	AV:N/AC:L/Au:N/C:C/I:C/A:C			
19	bash	4.2.50	5.2.15	CVE-2016-7543	Exact match		5.9 2017-09-13T08:53:25Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	7.5		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C		
20	bash	4.2.50	5.2.15	CVE-2019-18276	Exact match		3.8 2019-11-29T14:52:13Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	7.8		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C		
21	bash	4.2.50	5.2.15	CVE-2016-0634	Exact match		3.8 2017-08-24T16:24:21Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	5.2		AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C		
22	bash	4.2.50	5.2.15	CVE-2019-9924	Exact match		3.6 2019-03-22T15:28:31Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	7.6		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C		
23	bash	4.2.50	5.2.15	CVE-2022-3715	Exact match		3 2023-01-06T12:22:07Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	5.3		AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:P/RL:W/RC:C		
24	bash	4.2.50	5.2.15	CVE-2016-9401	Exact match		2.1 2017-01-23T21:59:00Z	2018-07-24T01:54:27Z	bash	sample_C	2bc290ff789dc098bc036543cf5829ccfa01daf65	5.3	AV:L/AC:L/Au:N/C:N/I:N/A:P	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H		
25	berkeleydb	5.3.28-11		CVE-2016-3418	Exact match		6.9 2016-04-21T11:00:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
26	berkeleydb	5.3.28-11		CVE-2016-0694	Exact match		6.9 2016-04-21T10:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
27	berkeleydb	5.3.28-11		CVE-2016-0692	Exact match		6.9 2016-04-21T10:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
28	berkeleydb	5.3.28-11		CVE-2016-0689	Exact match		6.9 2016-04-21T10:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
29	berkeleydb	5.3.28-11		CVE-2016-0682	Exact match		6.9 2016-04-21T10:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
30	berkeleydb	5.3.28-11		CVE-2017-3606	Exact match		4.4 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
31	berkeleydb	5.3.28-11		CVE-2017-3617	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
32	berkeleydb	5.3.28-11		CVE-2017-3616	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
33	berkeleydb	5.3.28-11		CVE-2017-3615	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
34	berkeleydb	5.3.28-11		CVE-2017-3614	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
35	berkeleydb	5.3.28-11		CVE-2017-3613	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
36	berkeleydb	5.3.28-11		CVE-2017-3612	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
37	berkeleydb	5.3.28-11		CVE-2017-3611	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
38	berkeleydb	5.3.28-11		CVE-2017-3610	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
39	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	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
40	berkeleydb	5.3.28-11		CVE-2017-3608	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
41	berkeleydb	5.3.28-11		CVE-2017-3607	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
42	berkeleydb	5.3.28-11		CVE-2017-3605	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
43	berkeleydb	5.3.28-11		CVE-2017-3604	Exact match		3.7 2017-04-24T19:59:00Z	2019-03-06T12:45:40Z	libdb-5.3.	sample_C	edfc715c728e691e47817da2467a9bdf3ee8b28	7	AV:L/AC:H/Au:N/C:P/I:P/A:P	AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
44	berkeleydb	5.3.28-11ubuntu0.1		CVE-2016-3418	Exact match		6.9 2016-04-21T11:00:00Z	2019-07-20T01:02:06Z	libdb-5.3.	sample_C	1baf6e753680a4a2e30de4267d7fdb780a58fa19;	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu
45	berkeleydb	5.3.28-11ubuntu0.1		CVE-2016-3418	Exact match		6.9 2016-04-21T11:00:00Z	2019-01-19T11:20:42Z	libdb-5.3.	sample_C	1baf6e753680a4a2e30de4267d7fdb780a58fa19;	7.8	AV:L/AC:L/Au:N/C:C/I:C/A:C	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		ubuntu

C2 vulnerabilities

Figure 59: C2 CVEs (Black Duck)

Sample C2 Code Sentry Scan Report Excerpts

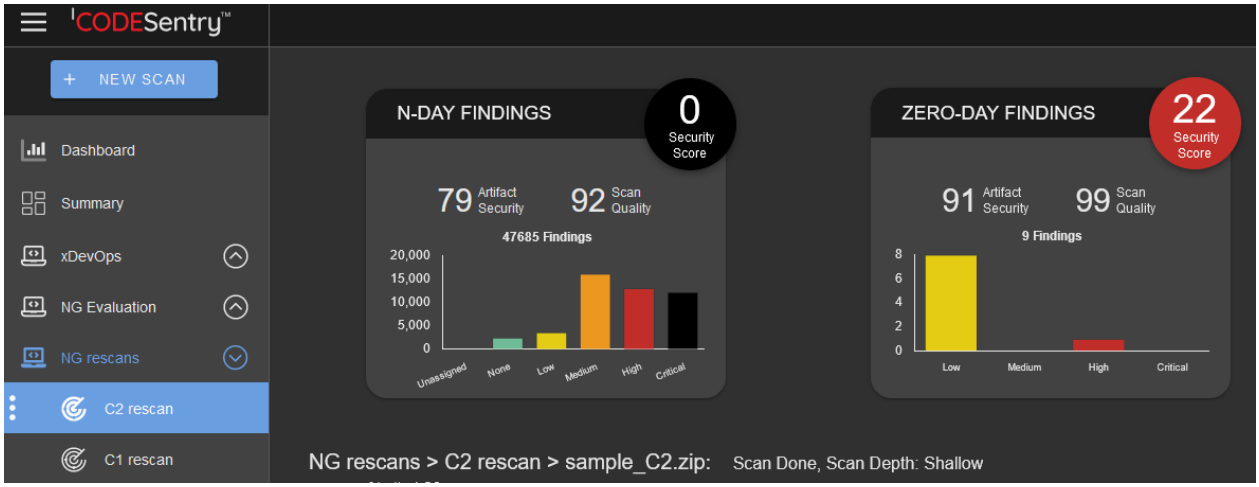


Figure 60: C2 Scan Overview (Code Sentry)

GRAMMATECH CODESentry

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/overlay2/21412d8b8dfb7184363222f85172f6472151235b3fd16317fe1e2e3744897c57/diff/home/weblmt/env/python_lib/dist-packages/ipaddress.pyc
aliyungo	20220907	unspecified	100	0	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/062b2df6984742207d8e00bca1f65689b37fc4f39427347ef81e76d0215ada47/diff/bin/registry
apache-http-server	agb_before_aaa_changes	unspecified	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/sbin/checkgid
apache2	upstream-2.4.27	unspecified	100	0	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/ab
apache_http_server	2.4.33	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/sbin/rotatelogs
apache_http_server	2.4.40	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/htpasswd
apache_http_server	2.4.48	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/sbin/htcacheclean
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/ab
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/htdbm
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/htdigest
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/httxt2dbm
apache_http_server	2.4.54	apache	32	1	NG rescans/C2 rescan/sample_C2.zip/VSWc2/NVMe/docker/overlay2/19f93c843662c21857ec5e20cbc323785e9c72dbfef9c54237b16ccf38594798/diff/usr/bin/logresolve

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

GRAMMATECH CODESentry

Zero-Day Findings

Findings for sample_C2.zip

Scan Depth: **Shallow**
MD5: **cc85e13f29d2a025a66c62ef25172e4a**

Top 25 CWE Findings

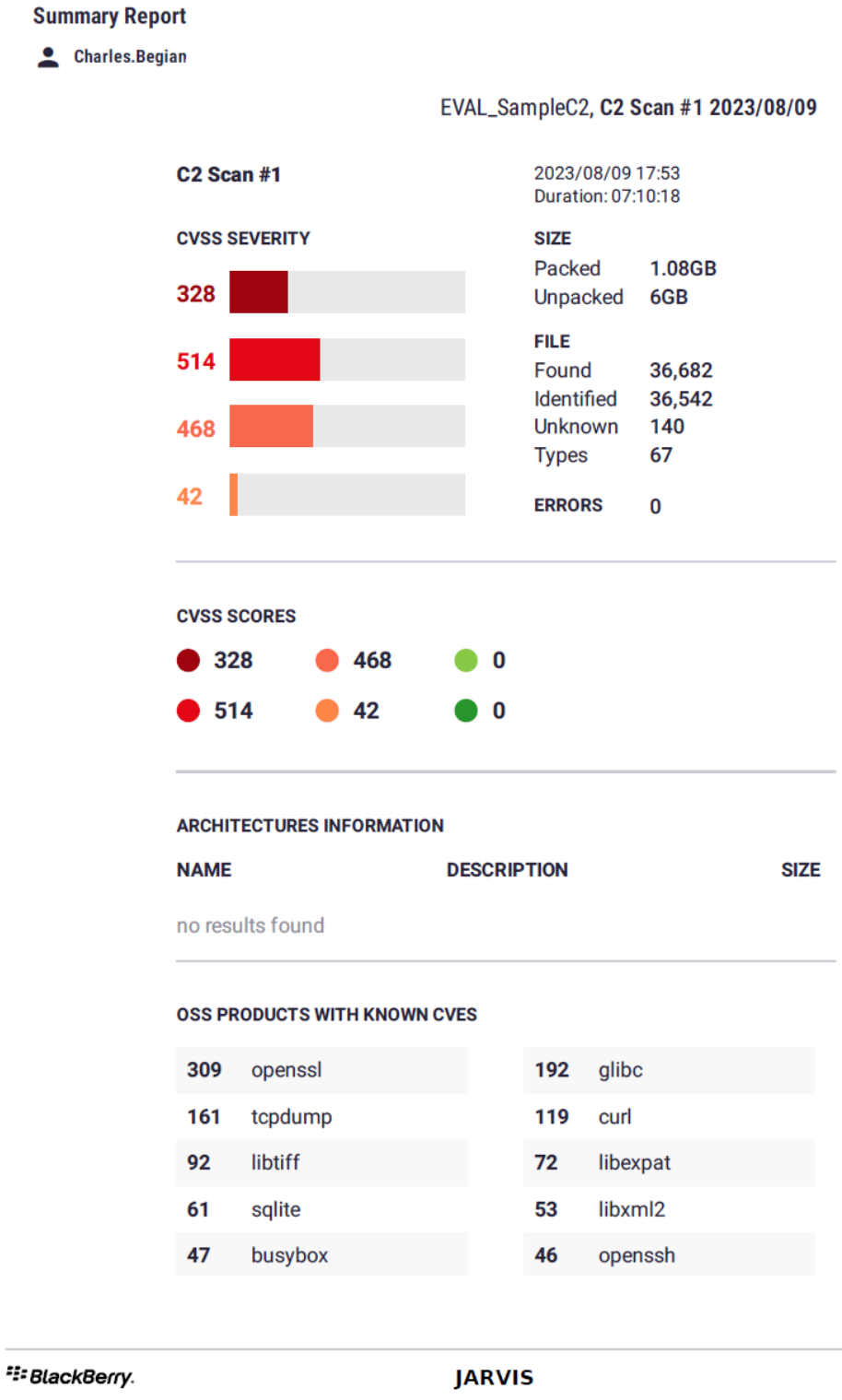
Rank	ID	Name	Instances
1	CWE:787	Out-of-bounds Write	-
2	CWE:79	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	-
3	CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0
4	CWE:20	Improper Input Validation	-
5	CWE:125	Out-of-bounds 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

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

Sample C2 Jarvis Scan Report Excerpts



Summary Report

Charles.Begian

EVAL_SampleC2, **C2 Scan #1 2023/08/09**

C2 Scan #1

2023/08/09 17:53
Duration: 07:10:18

CVSS SEVERITY

328
514
468
42

SIZE

Packed	1.08GB
Unpacked	6GB

FILE

Found	36,682
Identified	36,542
Unknown	140
Types	67

ERRORS 0

CVSS SCORES

328 468 0
514 42 0

ARCHITECTURES INFORMATION

NAME	DESCRIPTION	SIZE

no results found

OSS PRODUCTS WITH KNOWN CVES

309	openssl	192	glibc
161	tcpdump	119	curl
92	libtiff	72	libexpat
61	sqlite	53	libxml2
47	busybox	46	openssh

BlackBerry. JARVIS Created: 2023-04-

Figure 63: C2 Scan Overview (Jarvis)

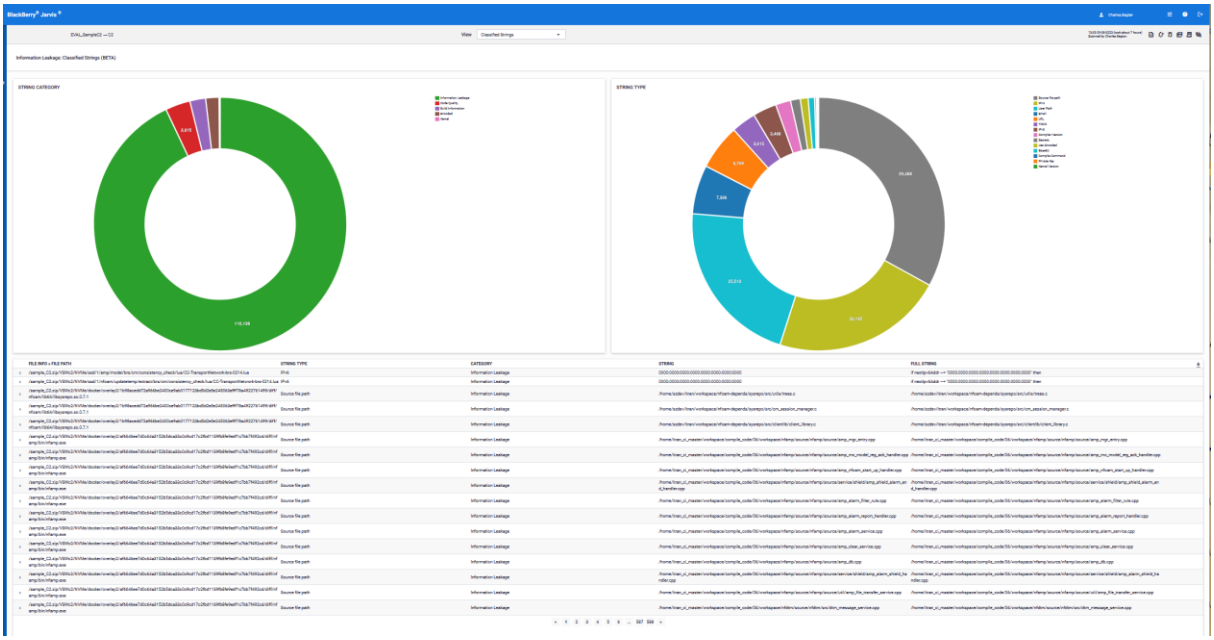


Figure 64: C2 Information Leakage (Jarvis)

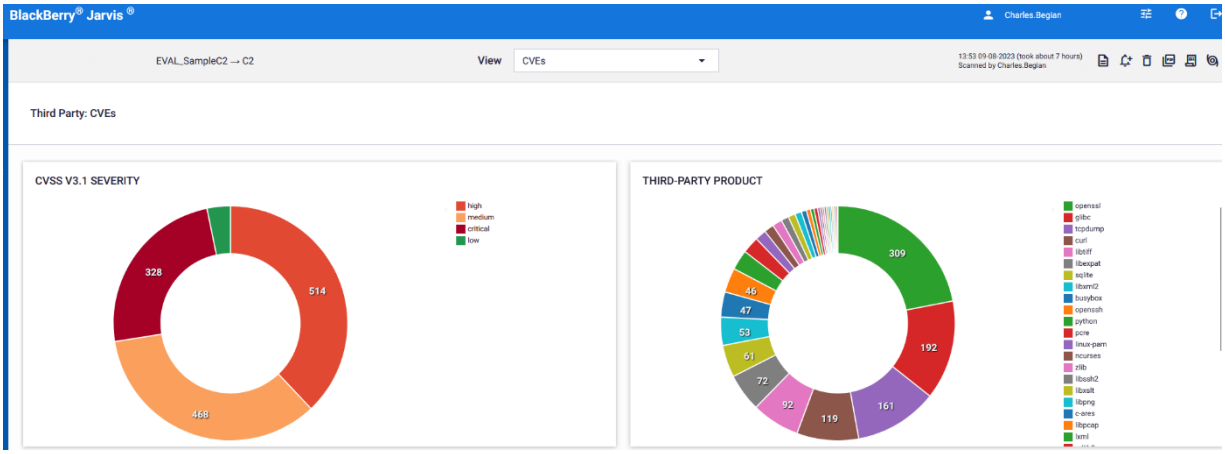


Figure 65: C2 CVSS Severity Report (Jarvis)

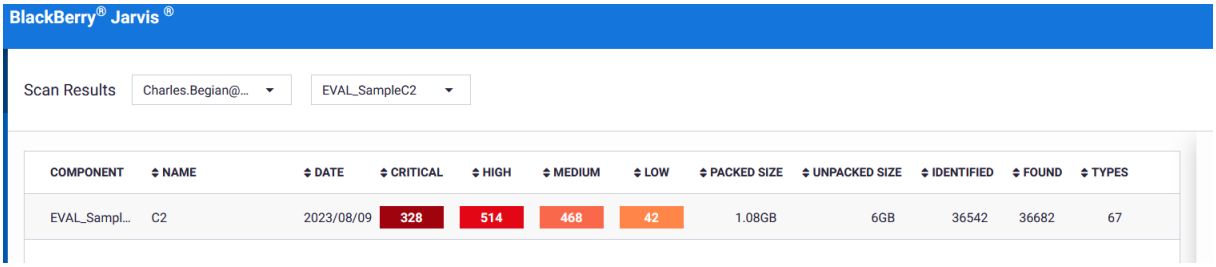


Figure 66: C2 CVE Summary by Severity (Jarvis)

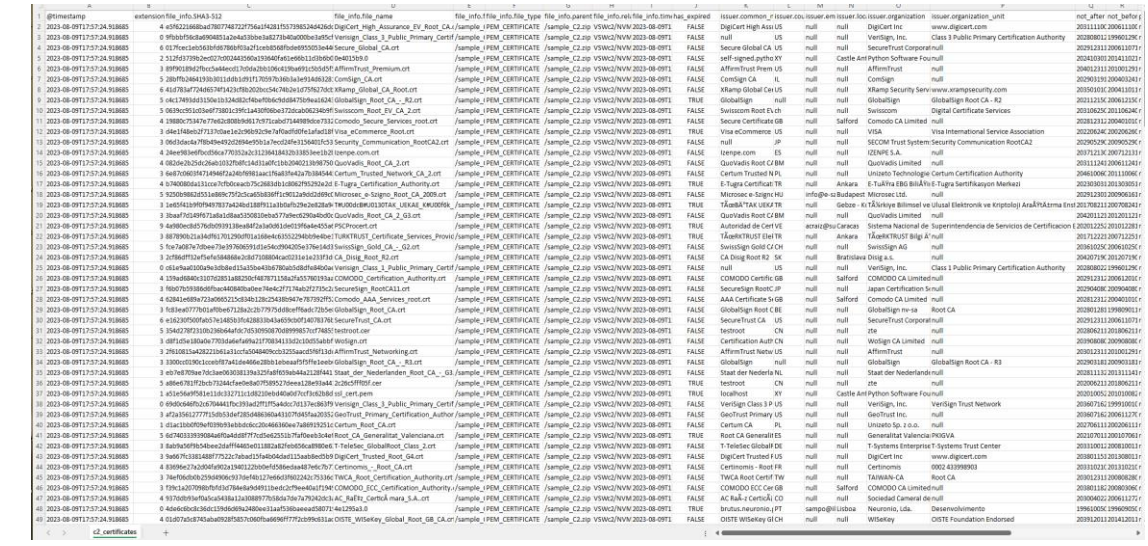


Figure 67: C2 Certificates report (Jarvis)

Figure 68: C2 CVEs (Jarvis)

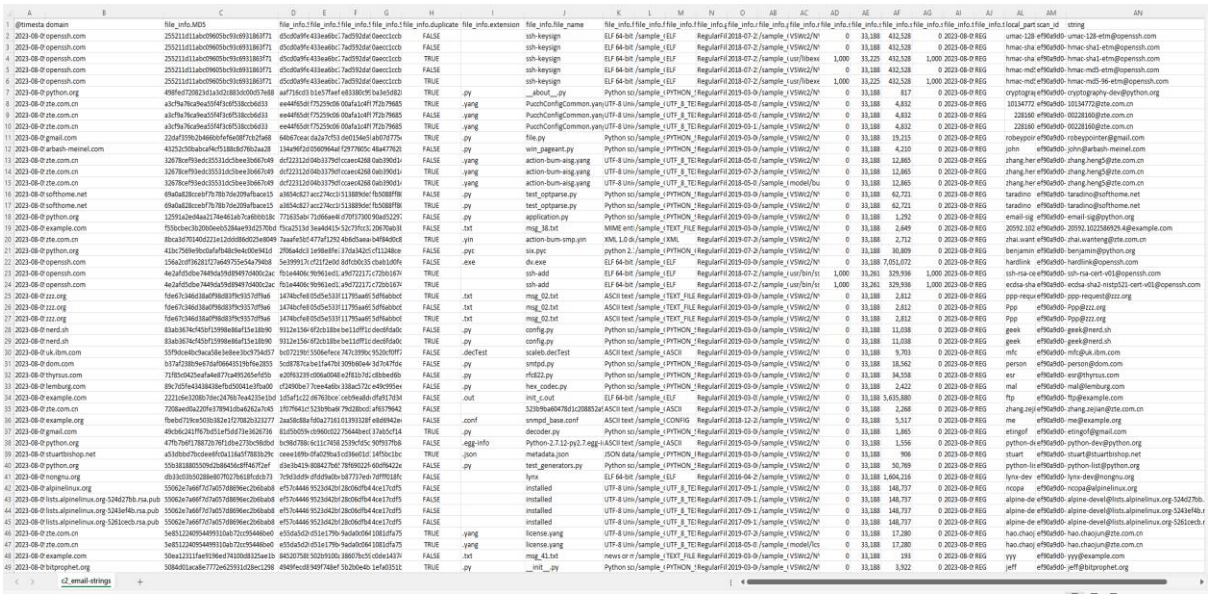


Figure 69: C2 email addresses (Jarvis)

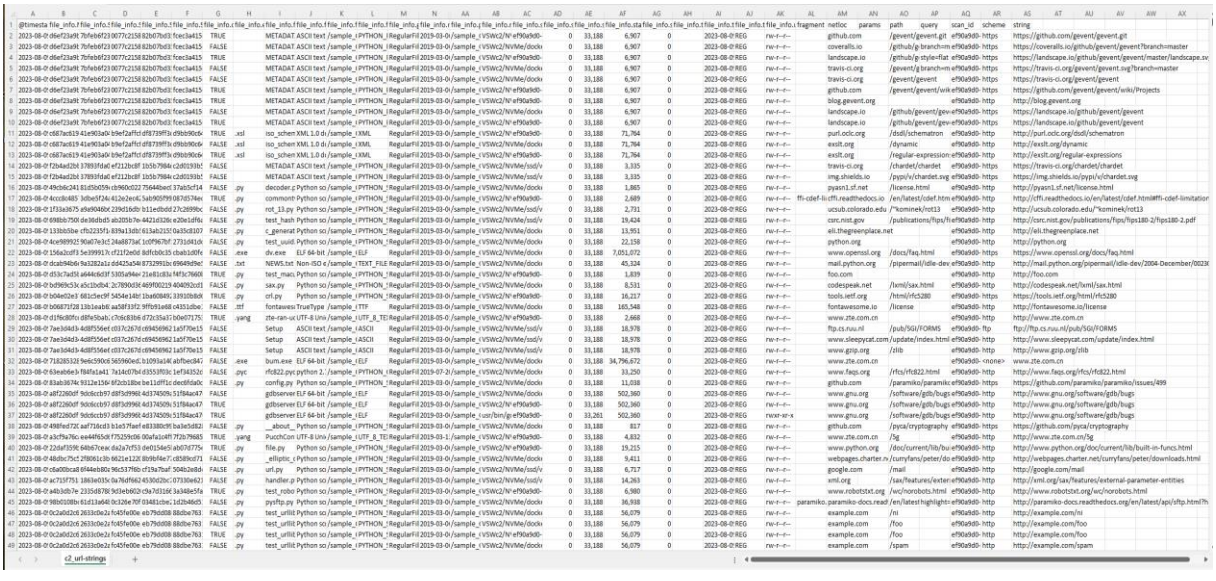


Figure 70: C2 URL Report (Jarvis)

Sample C2 Finite State Platform Scan Report Excerpts

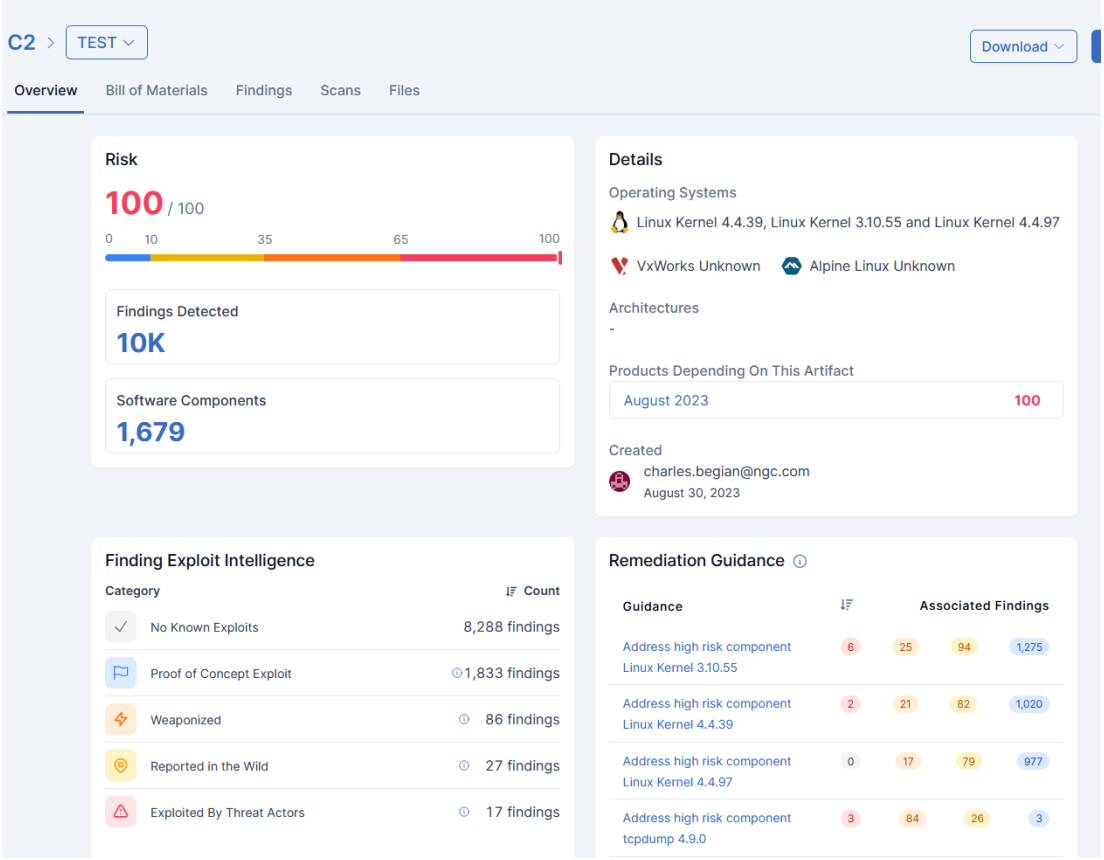


Figure 71: C2 Scan Overview (Finite State Platform)

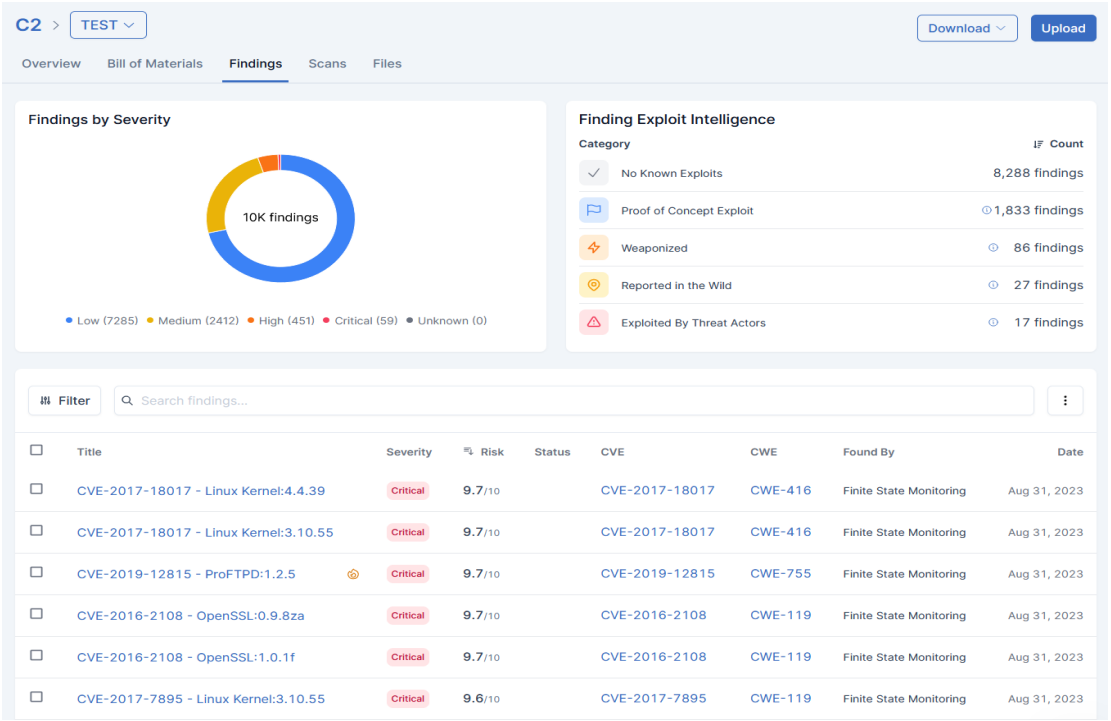


Figure 72: C2 Findings (Finite State Platform)

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	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

Figure 73: C2 Findings Categories (Finite State Platform)

A	B	C	D	G	H	I
vulnIdFromTool	riskScore	cvssV3Sco	cvssVectorString	affectedComponents	exploitCount	maxExploitMaturity
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-2016-8610	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-2016-6305	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-2016-7054	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	poc
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-2016-8610	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-2016-6305	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-2016-7054	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	poc
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	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-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	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:1.0.2k	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:1.0.2e	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:1.0.2e	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:1.0.2e	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:1.0.1f	1	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	OpenSSL:1.0.1f	3	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	54	weaponized
CVE-2015-0292	7.2			OpenSSL:1.0.1f	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-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	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:7.57.0	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:7.57.0	1	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	1	poc
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	expat:2.1.0	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:H/A:H	expat:2.1.0	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:H/A:H	expat:2.1.1	1	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:2.1.1	1	poc
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	expat:2.1.1	1	poc
CVE-2019-6974	7.4	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	6	poc
CVE-2014-3673	7.4	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	2	poc
CVE-2015-4004	7.5			Linux Kernel:3.10.55	1	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	1	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	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:3.10.55	1	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	39	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	Linux Kernel:3.10.55	1	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	1	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

C2_TEST.exploit-intel

Figure 74: C2 CVE Exploitability (Finite State Platform)

APPENDIX E: CST SCAN REPORT EXCERPTS FOR SAMPLE C3

Sample C3 Black Duck Scan Report Excerpts

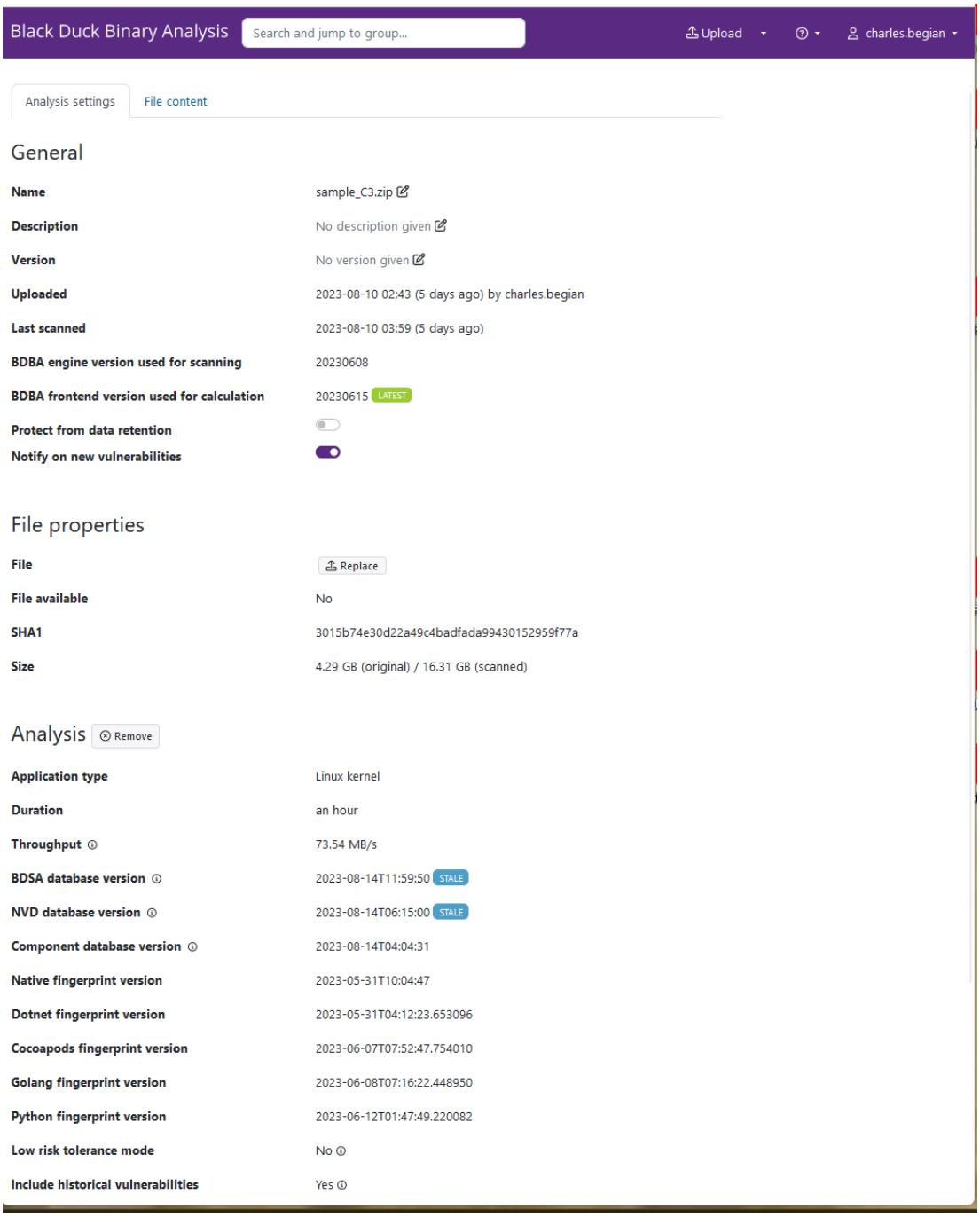
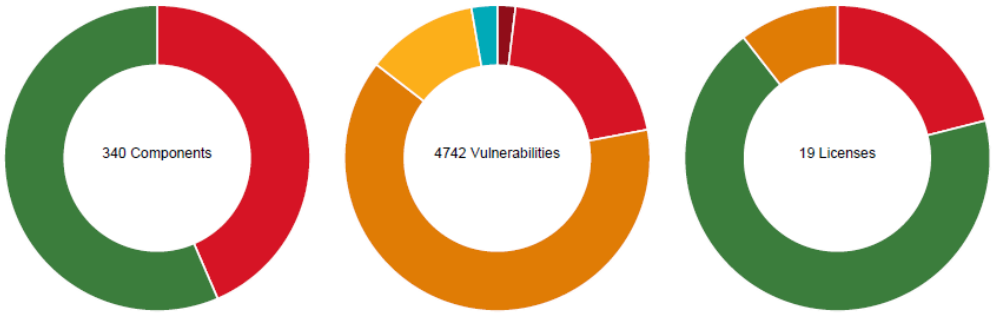


Figure 75: C3 Scan Overview (Black Duck)

Report generated 2023-08-13T23:27:28Z
https://protecode-sc.com/products/24698193

sample_C3.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY



Components	340
Vulnerable	148
No known vulnerabilities	192

Vulnerabilities	4742
Critical	91
High	953
Medium	3010
Low	559
None	0
CVSS v3 score missing	129

Licenses	19
Copyleft	4
Permissive	13
Weak Copyleft	2
Proprietary	0

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

Details

Original filename	
SHA1 checksum	3015b74e30d22a49c4badfada99430152959f77a
Original file size	4292.88 MB

Infoleak

Asymmetric keys:	1351

Report generated 2023-08-13T23:27:32Z
https://protecode-sc.com/products/24698193

AWS keys:	0
Custom pattern matches:	0
Emails:	15350
HTTP authentication:	0
Image metadata:	0
IP addresses:	14970
JSON web tokens:	0
MAC addresses:	184
OAuth tokens:	0
Passwords:	397
Shell history:	10
URLs:	10309
Twilio keys:	0
Google cloud keys:	0
Facebook access tokens:	0

Figure 77: C3 Information leaks (Black Duck)

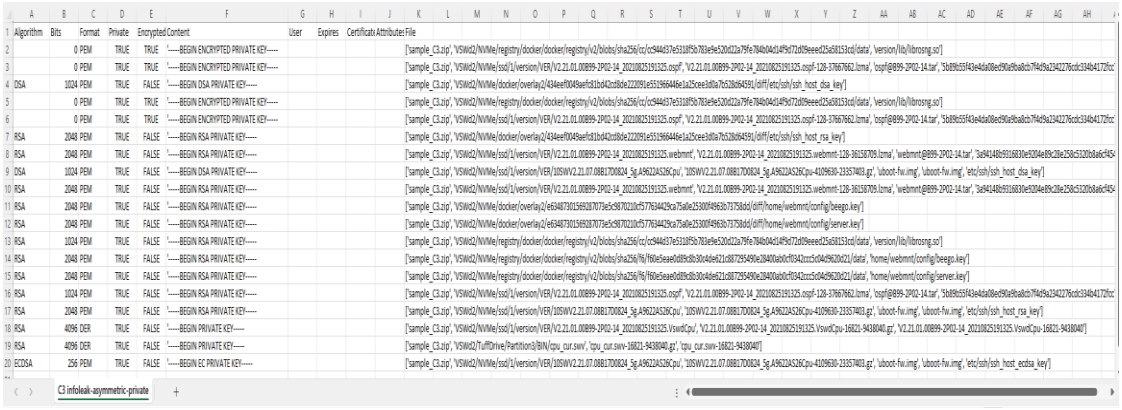


Figure 78: C3 Asymmetric keys (Black Duck)

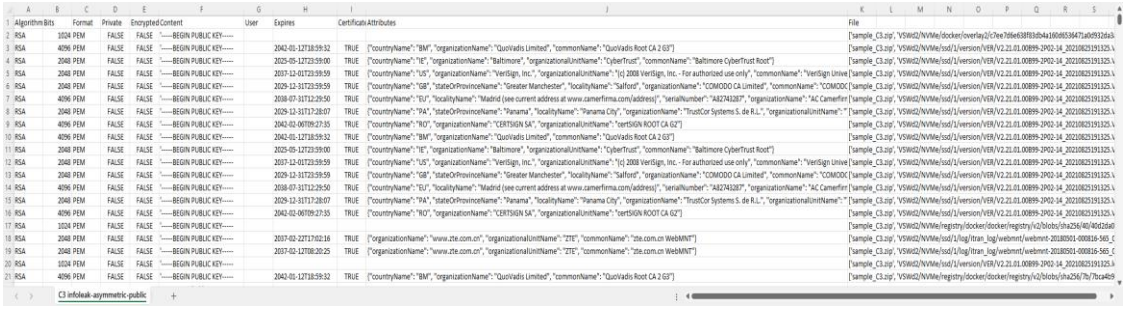
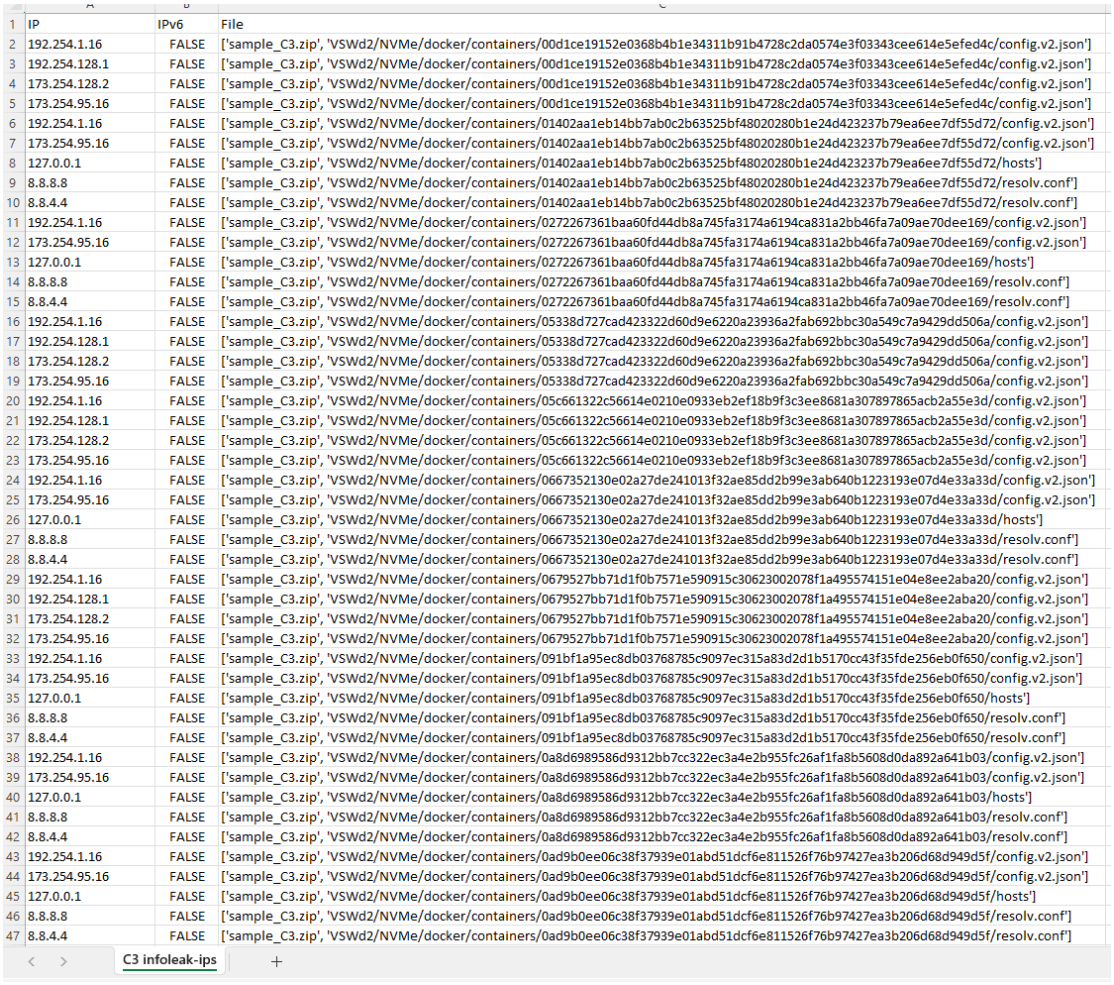


Figure 79: C3 Symmetric keys (Black Duck)

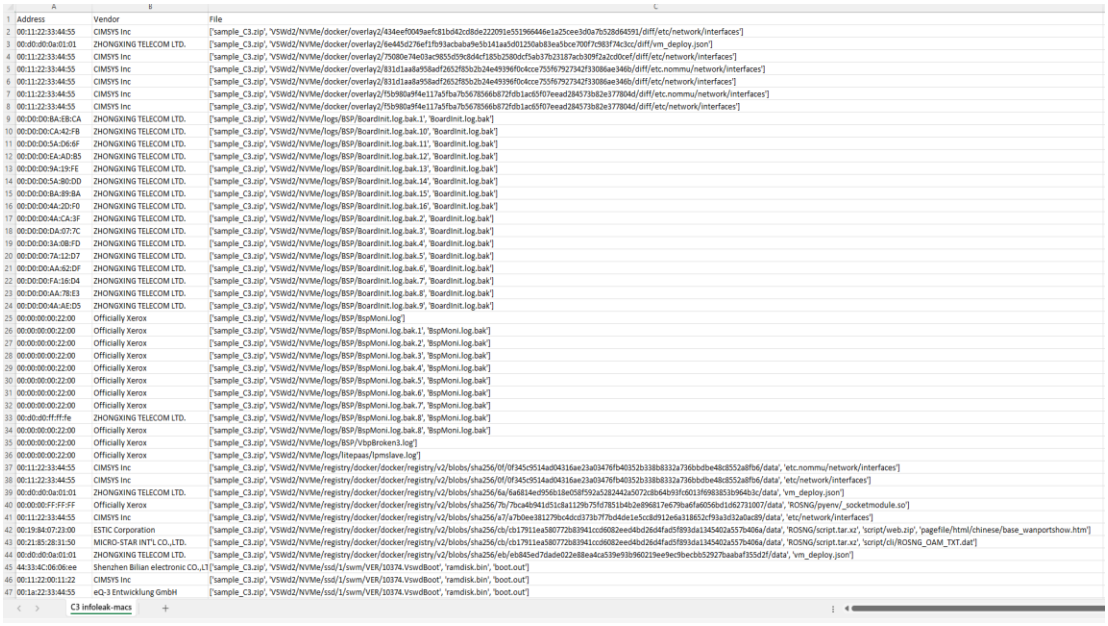
Figure 80: C3 Infoleak email addresses (Black Duck)



	IP	IPv6	File
2	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
3	192.254.128.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
4	173.254.128.2	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
5	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/00d1ce19152e0368b4b1e34311b91b4728c2da0574e3f03343cee614e5efed4c/config.v2.json']
6	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/config.v2.json']
7	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/config.v2.json']
8	127.0.0.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/hosts']
9	8.8.8.8	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/resolv.conf']
10	8.8.4.4	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/01402aa1eb14bb7ab0c2b63525bf48020280b1e24d423237b79ea6ee7df55d72/resolv.conf']
11	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db8a745fa3174a6194ca831a2bb46fa7a09ae70dee169/config.v2.json']
12	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db8a745fa3174a6194ca831a2bb46fa7a09ae70dee169/config.v2.json']
13	127.0.0.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db8a745fa3174a6194ca831a2bb46fa7a09ae70dee169/hosts']
14	8.8.8.8	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db8a745fa3174a6194ca831a2bb46fa7a09ae70dee169/resolv.conf']
15	8.8.4.4	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0272267361baa60fd44db8a745fa3174a6194ca831a2bb46fa7a09ae70dee169/resolv.conf']
16	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05338d727cad423322d60d9e6220a23936a2fab692bbc30a549c7a9429dd506a/config.v2.json']
17	192.254.128.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05338d727cad423322d60d9e6220a23936a2fab692bbc30a549c7a9429dd506a/config.v2.json']
18	173.254.128.2	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05338d727cad423322d60d9e6220a23936a2fab692bbc30a549c7a9429dd506a/config.v2.json']
19	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05338d727cad423322d60d9e6220a23936a2fab692bbc30a549c7a9429dd506a/config.v2.json']
20	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2ef18b9f3c3ee8681a307897865acb2a55e3d/config.v2.json']
21	192.254.128.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2ef18b9f3c3ee8681a307897865acb2a55e3d/config.v2.json']
22	173.254.128.2	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2ef18b9f3c3ee8681a307897865acb2a55e3d/config.v2.json']
23	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/05c661322c56614e0210e0933eb2ef18b9f3c3ee8681a307897865acb2a55e3d/config.v2.json']
24	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/config.v2.json']
25	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/config.v2.json']
26	127.0.0.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/hosts']
27	8.8.8.8	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/resolv.conf']
28	8.8.4.4	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0667352130e02a27de241013f32ae85dd2b99e3ab640b1223193e07d4e33a33d/resolv.conf']
29	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']
30	192.254.128.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0679527bb71d1f0b7571e590915c30623002078f1a495574151e04e8ee2aba20/config.v2.json']
31	173.254.128.2	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/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/hosts']
36	8.8.8.8	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']
37	8.8.4.4	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768785c9097ec315a83d2d1b5170cc43f35fde256eb0f650/resolv.conf']
38	192.254.1.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']
39	173.254.95.16	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/config.v2.json']
40	127.0.0.1	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/hosts']
41	8.8.8.8	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/resolv.conf']
42	8.8.4.4	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/0a8d6989586d9312bb7cc322ec3a4e2b955fc26af1fa8b5608d0da892a641b03/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/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']

C3 infoleak-ips

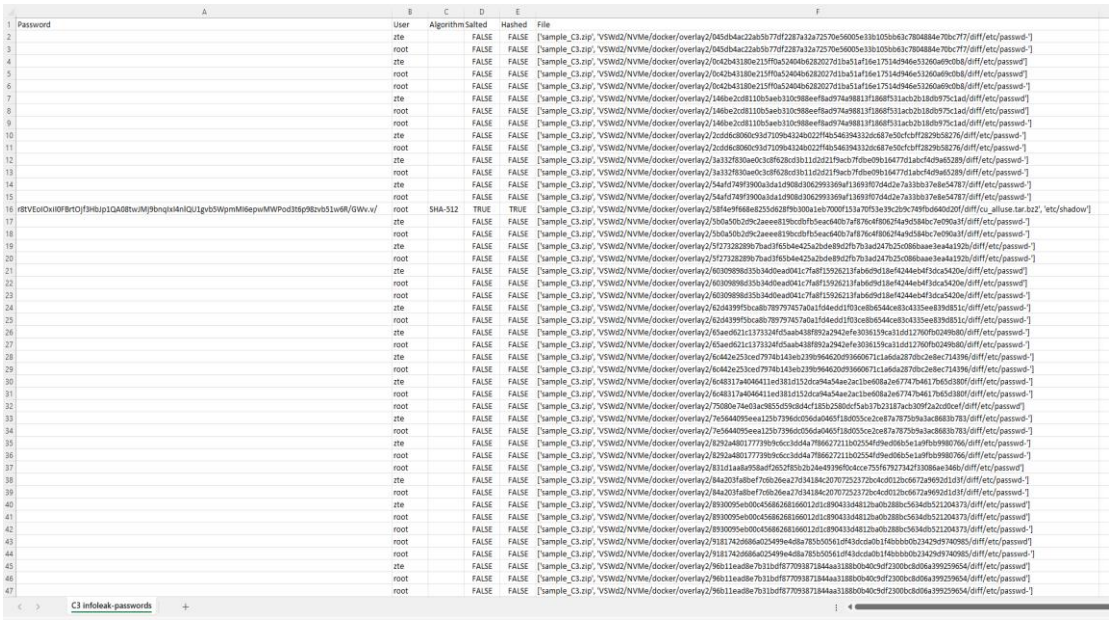
Figure 81: Infoleak IP addresses (Black Duck)



	Address	Vendor	File
2	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/434eef0049aefc81bd42cd8de222091e55196646e1a25cee3d0a7b528d64591/diff/etc/network/interfaces']
3	00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/6e445d276ef1fb93acbaba9e5b141aa5d01250ab83ea5bce700f7c983f74c3cc/diff/vm_deploy.json']
4	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75080e74e03ac9855d59c8d4cf185b2580dcf5ab37b23187acb309f2a2cd0cef/diff/etc/network/interfaces']
5	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/831d1aa8a958adf2652f85b2b24e49396f0c4cce755f67927342f330866ae346b/diff/etc.nommu/network/interfaces']
6	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/831d1aa8a958adf2652f85b2b24e49396f0c4cce755f67927342f330866ae346b/diff/etc/network/interfaces']
7	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/f5b980a9f4e117a5fba7b5678566b872fdb1ac65f07eead284573b82e377804d/diff/etc.nommu/network/interfaces']
8	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/f5b980a9f4e117a5fba7b5678566b872fdb1ac65f07eead284573b82e377804d/diff/etc/network/interfaces']
9	00:D0:D0:BA:EB:CA	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.1', 'BoardInit.log.bak']
10	00:D0:D0:CA:42:FB	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.10', 'BoardInit.log.bak']
11	00:D0:D0:5A:D6:6F	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.11', 'BoardInit.log.bak']
12	00:D0:D0:EA:AD:B5	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.12', 'BoardInit.log.bak']
13	00:D0:D0:9A:19:FE	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.13', 'BoardInit.log.bak']
14	00:D0:D0:5A:90:DD	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.14', 'BoardInit.log.bak']
15	00:D0:D0:BA:89:BA	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.15', 'BoardInit.log.bak']
16	00:D0:D0:4A:2D:F0	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.16', 'BoardInit.log.bak']
17	00:D0:D0:4A:CA:3F	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.2', 'BoardInit.log.bak']
18	00:D0:D0:DA:07:7C	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.3', 'BoardInit.log.bak']
19	00:D0:D0:3A:08:FD	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.4', 'BoardInit.log.bak']
20	00:D0:D0:7A:12:D7	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.5', 'BoardInit.log.bak']
21	00:D0:D0:AA:62:DF	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.6', 'BoardInit.log.bak']
22	00:D0:D0:FA:16:D4	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.7', 'BoardInit.log.bak']
23	00:D0:D0:AA:7B:E3	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.8', 'BoardInit.log.bak']
24	00:D0:D0:4A:AE:D5	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BoardInit.log.bak.9', 'BoardInit.log.bak']
25	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log']
26	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.1', 'BspMoni.log.bak']
27	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.2', 'BspMoni.log.bak']
28	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.3', 'BspMoni.log.bak']
29	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.4', 'BspMoni.log.bak']
30	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.5', 'BspMoni.log.bak']
31	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.6', 'BspMoni.log.bak']
32	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.7', 'BspMoni.log.bak']
33	00:d0:d0:ff:ff:fe	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.8', 'BspMoni.log.bak']
34	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/BspMoni.log.bak.8', 'BspMoni.log.bak']
35	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/BSP/VbpBroken3.log']
36	00:00:00:00:22:00	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/logs/litepaas/lpmslave.log']
37	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/0f/0f345c9514ad04316ae23a03476fb40352b338b8332a736bbdbe48c8552a8fb6/data', 'etc.nommu/network/interfaces']
38	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/0f/0f345c9514ad04316ae23a03476fb40352b338b8332a736bbdbe48c8552a8fb6/data', 'etc/network/interfaces']
39	00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/6a/6a6814ed956b18e058f592a528242a5072c8b64b93fc6013f6983853b964b3c/data', 'vm_deploy.json']
40	00:00:0F:FF:FF:FF	Officially Xerox	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/7b/7bca4b941d51c8a1129b75fd7851b4b2e896817e679ba6fa6056bd1d62731007/data', 'ROSNG/pyenv/_socketmodule.so']
41	00:11:22:33:44:55	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/a7/a7b0ee381279bc4dcd373b7f7bd4de1e5cc8d912e6a318652cf93a3d32a0ac89/data', 'etc/network/interfaces']
42	00:19:B4:07:23:00	ESTIC Corporation	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.tar.xz', 'script/web.zip', 'pagefile/html/chinese/base_wanportshow.htm']
43	00:21:85:28:31:50	MICRO-STAR INT'L CO.,LTD.	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/cb/cb17911ea580772b83941ccd6082eed4bd26d4fad5f893da1345402a557b406a/data', 'ROSNG/script.tar.xz', 'script/cli/ROSNG_OAM_TXT.dat']
44	00:d0:d0:0a:01:01	ZHONGXING TELECOM LTD.	['sample_C3.zip', 'VSWd2/NVMe/registry/docker/docker/registry/v2/blobs/sha256/eb/eb845ed7dade022e88ea4ca539e930960219ee9ec9becbb52927baabaf355d2f/data', 'vm_deploy.json']
45	44:33:4C:06:06:ee	Shenzhen Bilian electronic CO.,LTD	['sample_C3.zip', 'VSWd2/NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', 'boot.out']
46	00:11:22:00:11:22	CIMSYS Inc	['sample_C3.zip', 'VSWd2/NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', 'boot.out']
47	00:1a:22:33:44:55	eQ-3 Entwicklung GmbH	['sample_C3.zip', 'VSWd2/NVMe/ssd/1/swm/VER/10374.VswdBoot', 'ramdisk.bin', 'boot.out']

C3 infoleak-macs

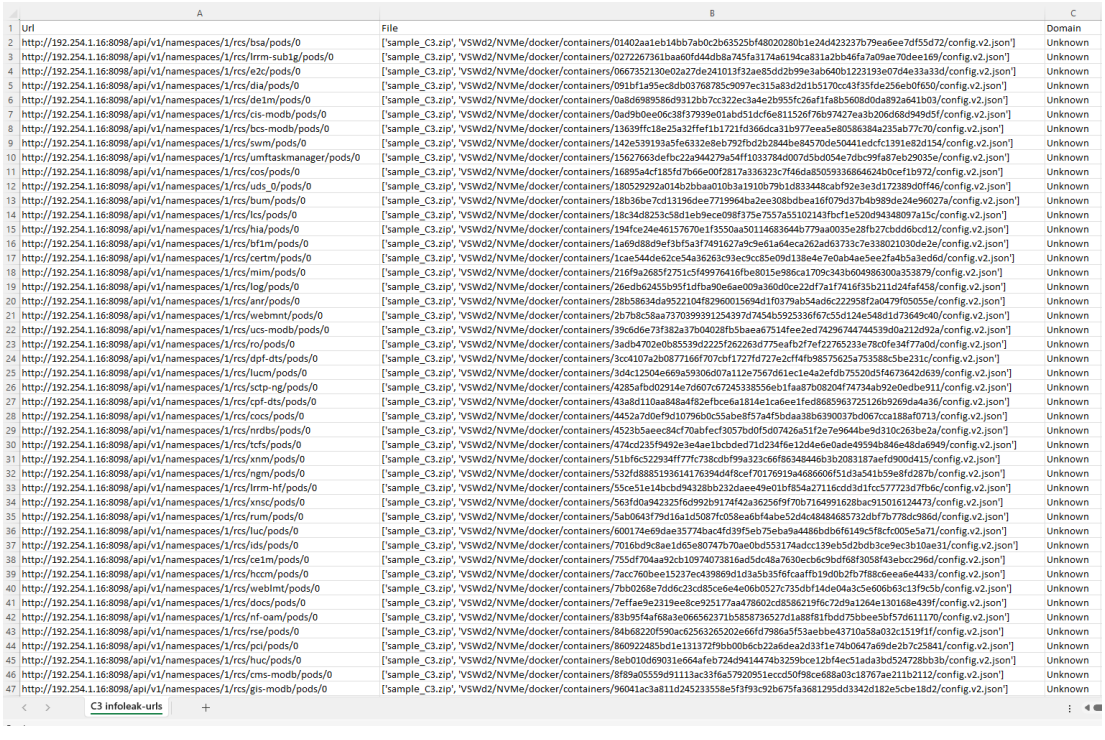
Figure 82: C3 Infoleak MAC addresses (Black Duck)



	A	B	C	D	E	F
1	Password	User	Algorithm	Salted	Hashed	File
2		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/045db4ac22ab5b77df2287a32a72570e56005e33b105bb63c7804884e70bc7f7/diff/etc/passwd-']
3		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/045db4ac22ab5b77df2287a32a72570e56005e33b105bb63c7804884e70bc7f7/diff/etc/passwd-']
4		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0a52404b628202 7d1ba51af16e17514d946e53260a69c0b8/diff/etc/passwd']
5		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0a52404b628202 7d1ba51af16e17514d946e53260a69c0b8/diff/etc/passwd-']
6		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0a52404b628202 7d1ba51af16e17514d946e53260a69c0b8/diff/etc/passwd-']
7		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/etc/passwd']
8		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/etc/passwd']
9		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/etc/passwd-']
10		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/2cdd6c8060c93d7109b4324b022ff4b546394332dc687e50cfcfbff2829b58276/diff/etc/passwd-']
11		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/2cdd6c8060c93d7109b4324b022ff4b546394332dc687e50cfcfbff2829b58276/diff/etc/passwd-']
12		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/3a332f830ae0c3c8f628cd3b11d2d21f9acb7fdbe09b16477d1abcf4d9a65289/diff/etc/passwd-']
13		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/3a332f830ae0c3c8f628cd3b11d2d21f9acb7fdbe09b16477d1abcf4d9a65289/diff/etc/passwd-']
14		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/54afd749f3900a3da1d908d3062993369af13693f07d4d2e7a33bb37e8e54787/diff/etc/passwd']
15		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/54afd749f3900a3da1d908d3062993369af13693f07d4d2e7a33bb37e8e54787/diff/etc/passwd-']
16	r8tVEoIOxii0FBrtOjf3Hbjp1QAGBtwJMjf9bnqIxI4nlQU1gvb5WpmMIi6epwMWPod3t6p98zvb51w6R/GWv.v/	root	SHA-512	TRUE	TRUE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/58f4e9f668e8255d628f9b3001eb7000f153a70f53e39c2b9c749fbd640d20f/diff/cu_alluse.tar.bz2', 'etc/shadow']
17		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5b0a50b2d9c2aeee819bcdbfb5eac640b7af876c4f80624fa9d584bc7e090a3f/diff/etc/passwd-']
18		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5b0a50b2d9c2aeee819bcdbfb5eac640b7af876c4f80624fa9d584bc7e090a3f/diff/etc/passwd-']
19		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5f273282289b7bad3f65b4e425a2bde89d2fb7b3ad247b25c086baae3ea4a192b/diff/etc/passwd-']
20		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/5f273282289b7bad3f65b4e425a2bde89d2fb7b3ad247b25c086baae3ea4a192b/diff/etc/passwd-']
21		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/60309898d35b34d0ead041c7fa8f15926213fab6d9d18ef4244eb4f3dca5420e/diff/etc/passwd']
22		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/60309898d35b34d0ead041c7fa8f15926213fab6d9d18ef4244eb4f3dca5420e/diff/etc/passwd']
23		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/60309898d35b34d0ead041c7fa8f15926213fab6d9d18ef4244eb4f3dca5420e/diff/etc/passwd-']
24		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/62d4399f5bca8b78979457a0a1fd4eddd1f03ce8b6544ce833 5ee839d851c/diff/etc/passwd']
25		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/62d4399f5bca8b78979457a0a1fd4eddd1f03ce8b6544ce833 5ee839d851c/diff/etc/passwd-']
26		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/65aed621c137332fd5aab438f892a2942efe3036159ca31dd12760fb0249b80/diff/etc/passwd']
27		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/65aed621c137332fd5aab438f892a2942efe3036159ca31dd12760fb0249b80/diff/etc/passwd-']
28		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/6c442e253ced7974b143eb2390f964620d936606f71c1a66a287dbc2e8ec714396/diff/etc/passwd']
29		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/6c442e253ced7974b143eb2390f964620d936606f71c1a66a287dbc2e8ec714396/diff/etc/passwd-']
30		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/6c48317a4046411ed381d152dcaf94a54ae2ac1be608a2e6774b4617b65d380f/diff/etc/passwd']
31		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/6c48317a4046411ed381d152dcaf94a54ae2ac1be608a2e6774b4617b65d380f/diff/etc/passwd-']
32		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/75080e74e03ac9855d59c8d4cf185b2580dcf5ab37b23187acb309f2a2cd0cef/diff/etc/passwd']
33		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/7e5644095eea125b7396dc056da0465f18d055ce2ce87a7875b9a3ac8683b783/diff/etc/passwd-']
34		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/7e5644095eea125b7396dc056da0465f18d055ce2ce87a7875b9a3ac8683b783/diff/etc/passwd-']
35		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8292a480177739b9c6cc3dd4a7f86627211b02554fd9ed06b5e1af9bb9980766/diff/etc/passwd']
36		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8292a480177739b9c6cc3dd4a7f86627211b02554fd9ed06b5e1af9bb9980766/diff/etc/passwd-']
37		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/831d1aa8a958adf2652f85b2b24e49396f0c4cce755f67927342f33086ae346b/diff/etc/passwd']
38		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/84a203fa8bef7c6b26ea27d34184c20707252372bc4cd012bc6672a9692d1d3f/diff/etc/passwd-']
39		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/84a203fa8bef7c6b26ea27d34184c20707252372bc4cd012bc6672a9692d1d3f/diff/etc/passwd-']
40		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8930095eb00c45686268166012d1c890433d4812ba0b288bc5634db521204373/diff/etc/passwd']
41		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8930095eb00c45686268166012d1c890433d4812ba0b288bc5634db521204373/diff/etc/passwd']
42		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/8930095eb00c45686268166012d1c890433d4812ba0b288bc5634db521204373/diff/etc/passwd-']
43		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/9181742d68ba025499e4d8a785b50561df43dcda0b1f4bbbb0b23429d9740985/diff/etc/passwd']
44		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/9181742d68ba025499e4d8a785b50561df43dcda0b1f4bbbb0b23429d9740985/diff/etc/passwd-']
45		zte		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/96b11ead8e7b31bdf87709387184 4aa3188b0b40c9df2300bc8d06a399259654/diff/etc/passwd']
46		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/96b11ead8e7b31bdf87709387184 4aa3188b0b40c9df2300bc8d06a399259654/diff/etc/passwd']
47		root		FALSE	FALSE	['sample_C3.zip', 'VSWd2/NVMe/docker/overlay2/96b11ead8e7b31bdf87709387184 4aa3188b0b40c9df2300bc8d06a399259654/diff/etc/passwd-']

C3 infoleak-passwords

Figure 83; C3 Infoleak passwords (Black Duck)



	A	B	C
1	Url	File	Domain
2	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']	Unknown
3	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']	Unknown
4	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']	Unknown
5	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/dia/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/091bf1a95ec8db03768 75c9097ec315a83d2d1b5170cc43f35fde256eb0f650/config.v2.json']	Unknown
6	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']	Unknown
7	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']	Unknown
8	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/bcs-modb/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/13639ffc18e25a32ffef1b1721fd366dca31b977eea5e80586384a225ab77c70/config.v2.json']	Unknown
9	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']	Unknown
10	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']	Unknown
11	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']	Unknown
12	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']	Unknown
13	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']	Unknown
14	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']	Unknown
15	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']	Unknown
16	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']	Unknown
17	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']	Unknown
18	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/mim/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/216f9a2685f2751c5f49976416fbe8015e986ca1709c343b6049863004353879/config.v2.json']	Unknown
19	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']	Unknown
20	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/anr/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/28b58634da9522104f8296001569 4d1f0379ab54ad6c222958f2a0479f05055e/config.v2.json']	Unknown
21	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/webmnt/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/2b7b8c58aa73703993912543 97d7454b5925336f67c55d124e548d1d73649c40/config.v2.json']	Unknown
22	http://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']	Unknown
23	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/ro/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/3adb4702e0b85539d2225f262263d775eafb2f7ef22765233e78c0fe34f77a0d/config.v2.json']	Unknown
24	http://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']	Unknown
25	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']	Unknown
26	http://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']	Unknown
27	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cpf-dts/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/43a8d110aa848a4f82efbce6a1814e1ca6ee1fed868596372512 6b9269da4a36/config.v2.json']	Unknown
28	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cocs/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/4452a7d0ef9d10796b0c55abe8f57a4f5bdaa38b6390037bd067cca188af0713/config.v2.json']	Unknown
29	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/nrdbs/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/4523b5aeec84cf70abfecf3057bd0f5d07426a51f2e7e9644be9d310c263be2a/config.v2.json']	Unknown
30	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']	Unknown
31	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']	Unknown
32	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/ngm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/532fd88851936141763 94d4f8cef70176919a4686606f51d3a541b59e8fd287b/config.v2.json']	Unknown
33	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/lrrm-hf/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/55ce51e14bcbd94328bb232daeee49e01bf854a27116cdd3d1fcc577723d7fb6c/config.v2.json']	Unknown
34	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']	Unknown
35	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/rum/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/5ab0643f79d16a1d5087fc058ea6bf4abe52d4c4848468573 2dbf7b778dc986d/config.v2.json']	Unknown
36	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/luc/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/600174e69dae35774bac4fd39f5eb75eba9a4486bdb6f6149c5f8cfc005e5a71/config.v2.json']	Unknown
37	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/ids/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/7016bd9c8ae1d65e80747b70ae0bd553174adcc139eb5d2bdb3ce9ec3b10ae31/config.v2.json']	Unknown
38	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/ce1m/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/755df704aa92cb10974037816ad5dc48a7630ecb6c9bdf68f3058f43ebcc296d/config.v2.json']	Unknown
39	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/hccm/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/7acc760bee15237ec439869d1d3a5b35f6fcaaffb19d0b2fb7f88c6eea6e4433/config.v2.json']	Unknown
40	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/weblmt/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/7bb0268e7dd6c23cd85ce6e4e06b0527c735dbf14de04a3c5e606b63c13f9c5b/config.v2.json']	Unknown
41	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/docs/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/7effae9e2319ee8ce925177aa478602cd8586219f6c72d9a1264e130168e439f/config.v2.json']	Unknown
42	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/nf-oam/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/83b954fa468a3e066562371b5858736527d1a88f81fbdd75bbeee5bf57d611170/config.v2.json']	Unknown
43	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/rse/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/84b68220f590ac62563265202e66fd7986a5f53aebbe43710a58a032c1519f1f/config.v2.json']	Unknown
44	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/pci/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/860922485bd1e131372f9bb00b6cb22a6dea2d33f1e74b0647a69de2b7c25841/config.v2.json']	Unknown
45	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/huc/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/8eb010d69031e664afeb724d94144749b3259bce12bf4ec51ada3bd524728bb3b/config.v2.json']	Unknown
46	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/cms-modb/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/8f89a05559d91113ac33f6a57920951eccd50f98ce688a03c18767ae211b2112/config.v2.json']	Unknown
47	http://192.254.1.16:8098/api/v1/namespaces/1/rcs/gis-modb/pods/0	['sample_C3.zip', 'VSWd2/NVMe/docker/containers/96041ac3a811d245233558e5f3f93c92b675fa3681295dd3342d182e5cbe18d2/config.v2.json']	Unknown

C3 infoleak-urls

Figure 84: C3 Infoleak URLS (Black Duck)

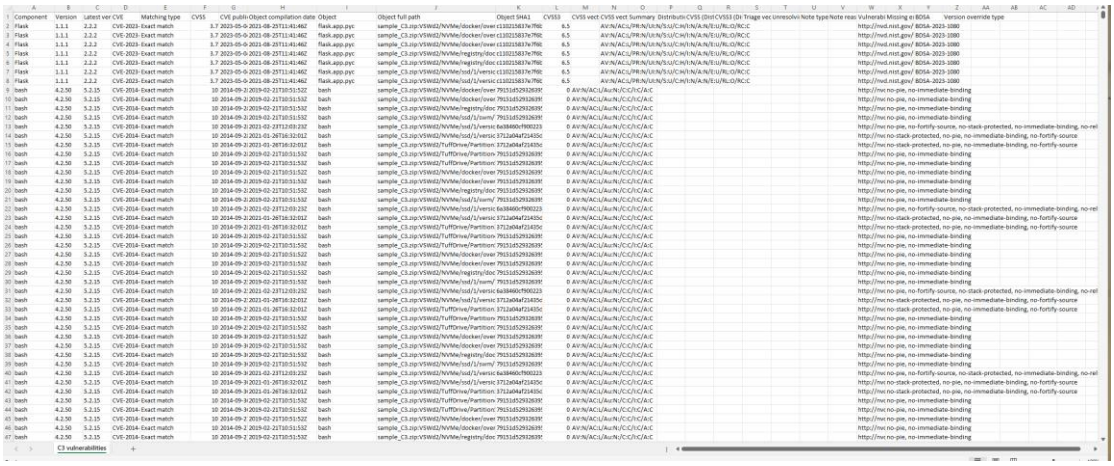


Figure 85: C3 CVEs (Black Duck)

Sample C3 Code Sentry Scan Report Excerpts

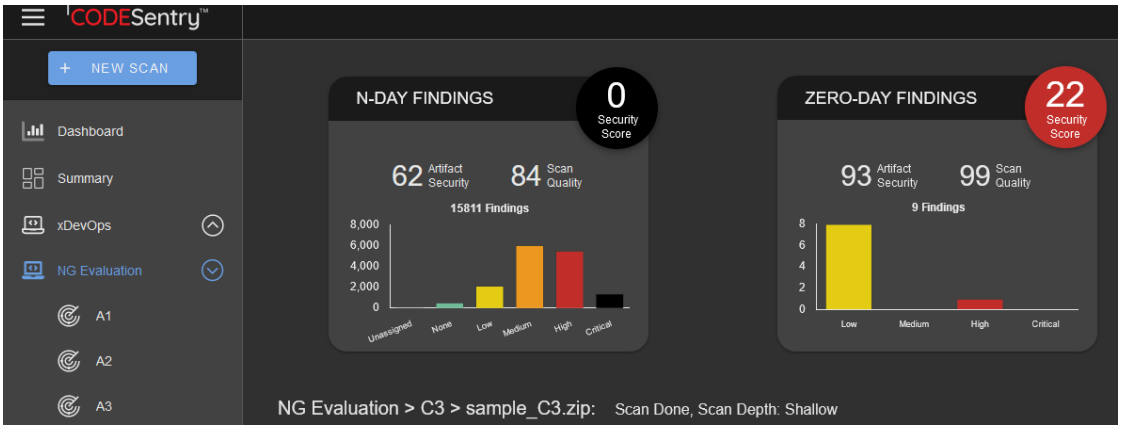


Figure 86: C3 Scan Overview (Code Sentry)

GRAMMATECH

CODESentry

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/d7cc9189a6da87d7c25d6b1a85a3a662c0968d4574c605cca18b3f92a1b8e69d/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/4cfdbc31c66f53f0fa85cf0d62fb6ae00c2aae20241ecf4b034aa332320efda0/data
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/0c224b9e36240bea2af020051a342f2cc35ec58864d7702aabb71f82cd587e88/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/0c224b9e36240bea2af020051a342f2cc35ec58864d7702aabb71f82cd587e88/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/0c42b43180e215ff0a52404b6282027d1ba51af16e17514d946e53260a69c0b8/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/146be2cd8110b5aeb310c988eef8ad974a98813f1868f531acb2b18db975c1ad/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/496a068cf5f40ebf1c53923733574f8499f8b843172a00c89ae15ef1256fcbe1/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/496a068cf5f40ebf1c53923733574f8499f8b843172a00c89ae15ef1256fcbe1/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/60309898d35b34d0ead041c7fa8f15926213fab6d9d18ef4244eb4f3dca5420e/diff/ordinaryuserhome/setfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/876db3a77b236e035d4131e9bec65cf1da8ca15f7c4fd38252110c787bd825a0/diff/ordinaryuserhome/getfacl
acl	2.2.52	unspecified	100	0	NG Evaluation/C3/sample_C3.zip/VSWd2/NVMe/docker/overlay2/8930095eb00c45686268166012d1c890433d4812ba0b288bc5634db521204373/diff/ordinaryuserhome/setfacl

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

GRAMMATECH

CODESentry

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.zip/VSWd2/TuffDrive/Partition4/ramdisk.bin**
Component ID: 9967864f-5b3b-4a68-820f-9ee6006dd6ac
Score Distribution: Unassigned: 0 None: 26 Low: 267 Medium: 813 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...

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

GRAMMATECH CODESentry

Zero-Day Findings

Findings for sample_C3.zip

Scan Depth: **Shallow**
MD5: **006198a09104c8f5f197a5407512ec8b**

Top 25 CWE Findings

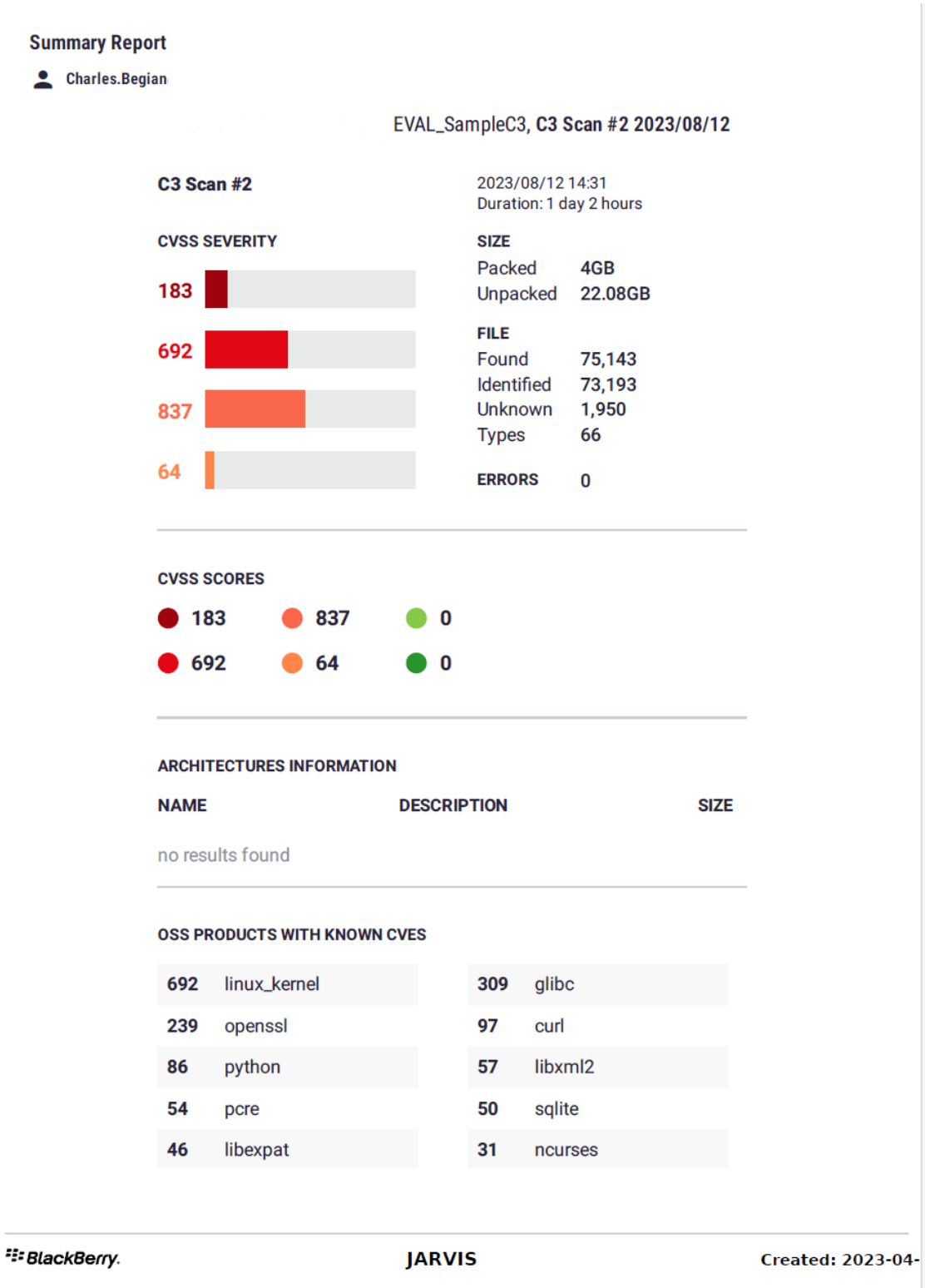
Rank	ID	Name	Instances
1	CWE:787	Out-of-bounds Write	-
2	CWE:79	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")	-
3	CWE:89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0
4	CWE:20	Improper Input Validation	-
5	CWE:125	Out-of-bounds 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

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

Sample C3 Jarvis Scan Report Excerpts



Summary Report

Charles.Begian

EVAL_SampleC3, **C3 Scan #2 2023/08/12**

C3 Scan #2

2023/08/12 14:31
Duration: 1 day 2 hours

CVSS SEVERITY

183
692
837
64

SIZE

Packed	4GB
Unpacked	22.08GB

FILE

Found	75,143
Identified	73,193
Unknown	1,950
Types	66

ERRORS 0

CVSS SCORES

183	837	0
692	64	0

ARCHITECTURES INFORMATION

NAME	DESCRIPTION	SIZE

no results found

OSS PRODUCTS WITH KNOWN CVES

692	linux_kernel	309	glibc
239	openssl	97	curl
86	python	57	libxml2
54	pcre	50	sqlite
46	libexpat	31	ncurses

BlackBerry. JARVIS Created: 2023-04-

Figure 90: C3 Scan Overview (Jarvis)

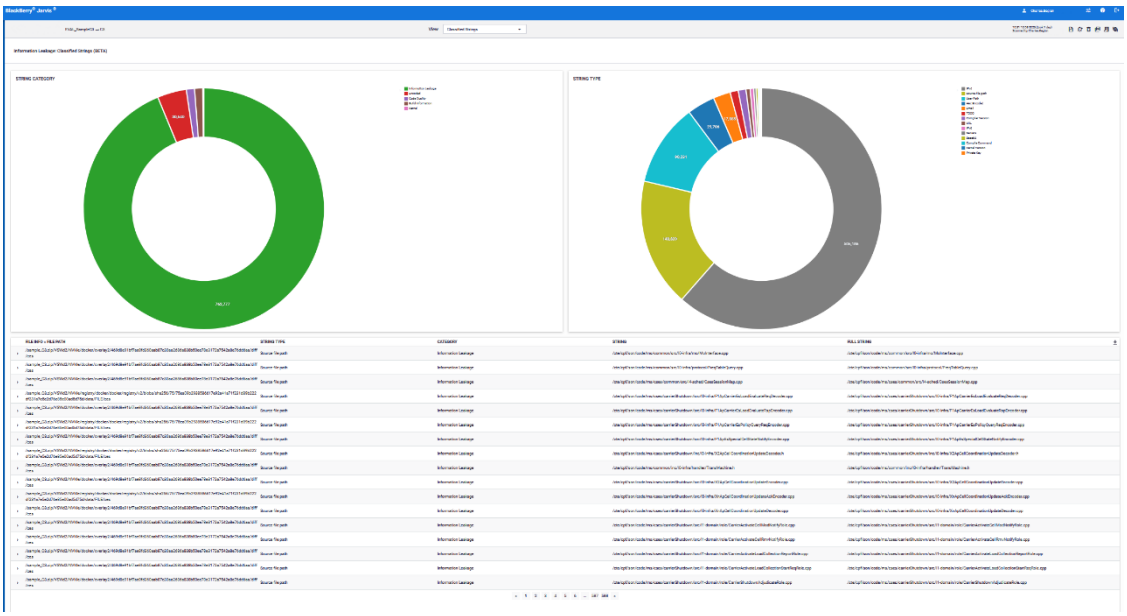


Figure 91: C3 Information Leakage (Jarvis)

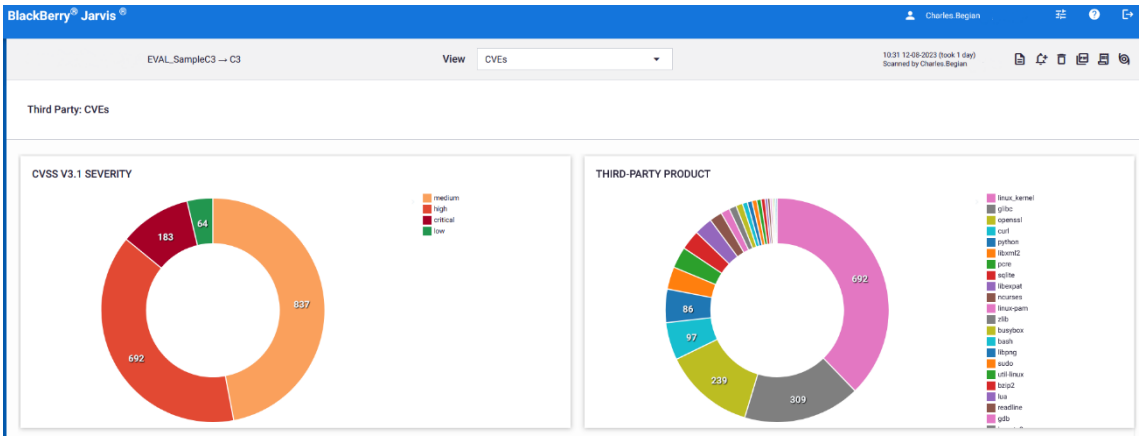


Figure 92: C3 CVSS Severity Report (Jarvis)

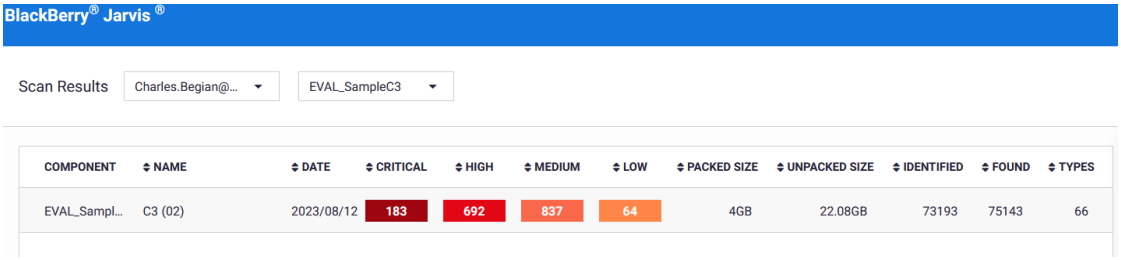


Figure 93: C3 CVE Summary by Severity (Jarvis)

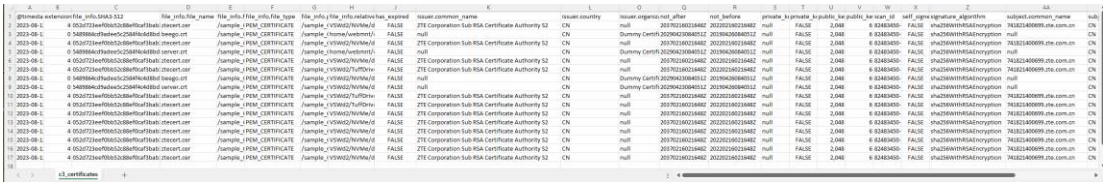


Figure 94: C3 Certificates Report (Jarvis)

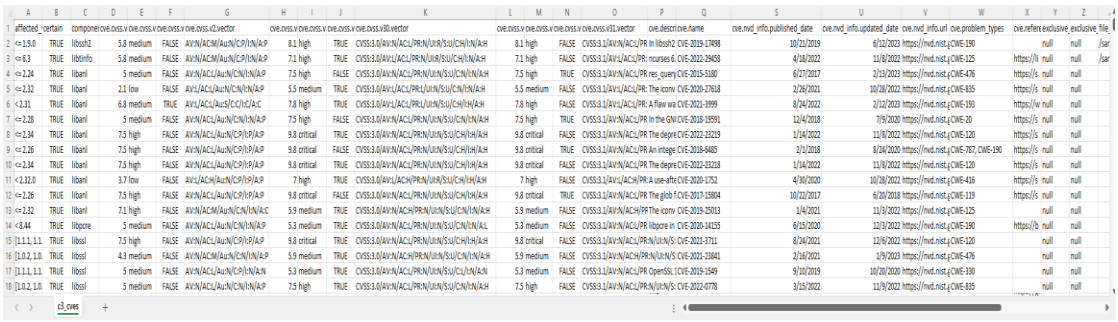


Figure 95: C3 CVEs (Jarvis)

Figure 96: C3 email addresses (Jarvis)

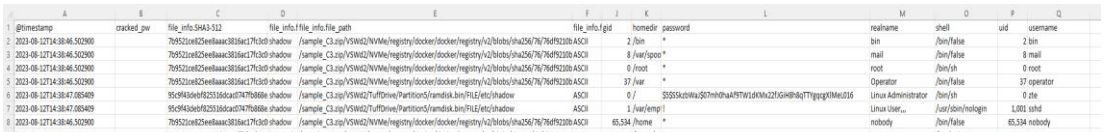


Figure 97: C3 Password File Analysis (Jarvis)

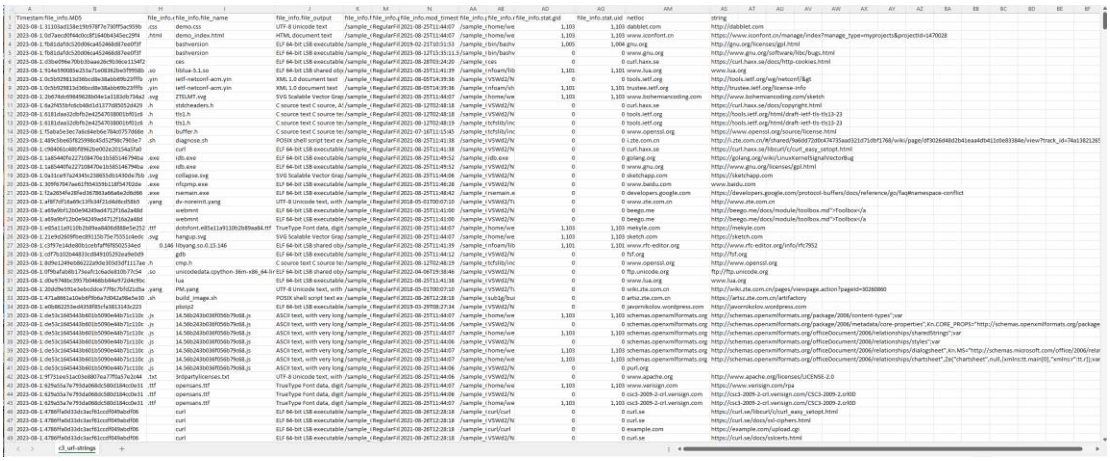


Figure 98: C3 Infoleak URL Report (Jarvis)

Sample C3 Finite State Platform Scan Report Excerpts

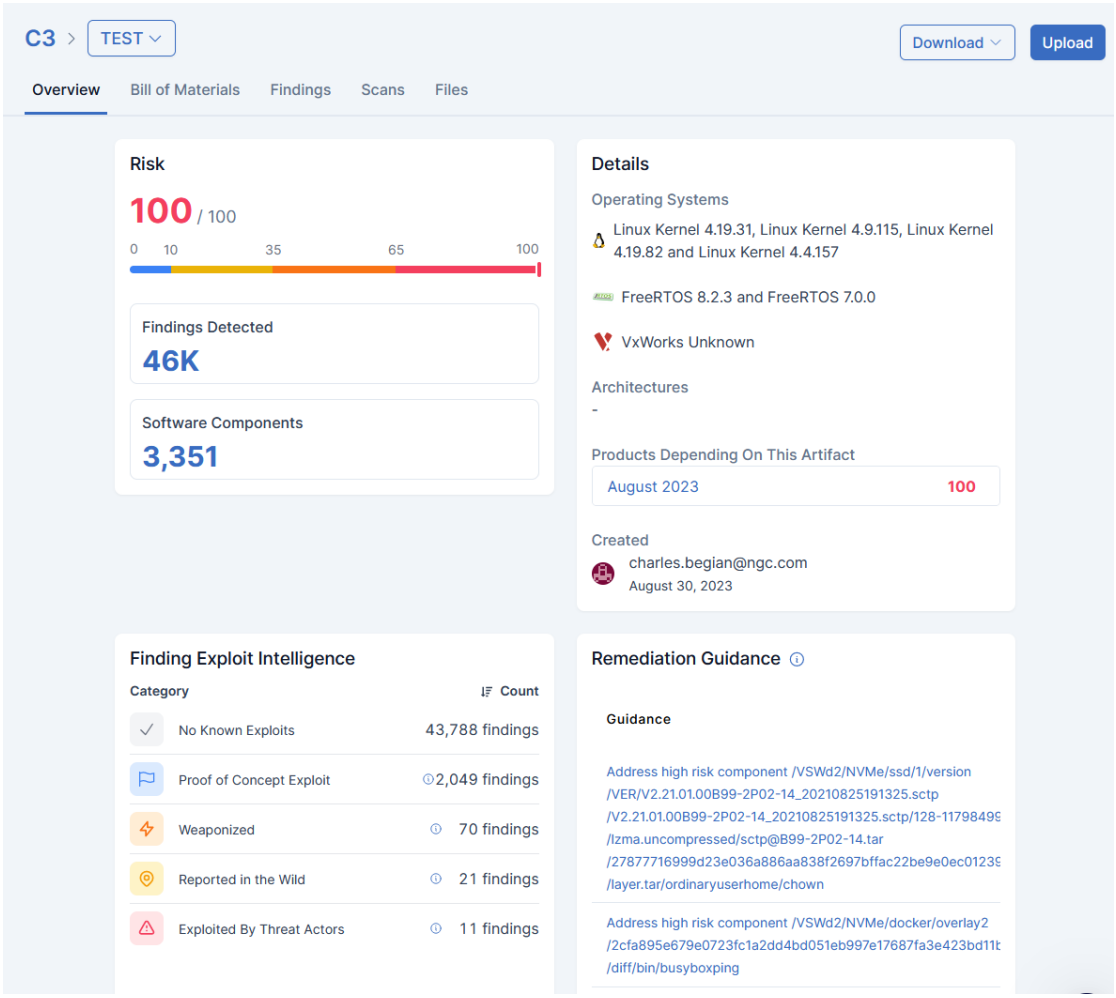


Figure 99: C3 Scan Overview (Finite State Platform)

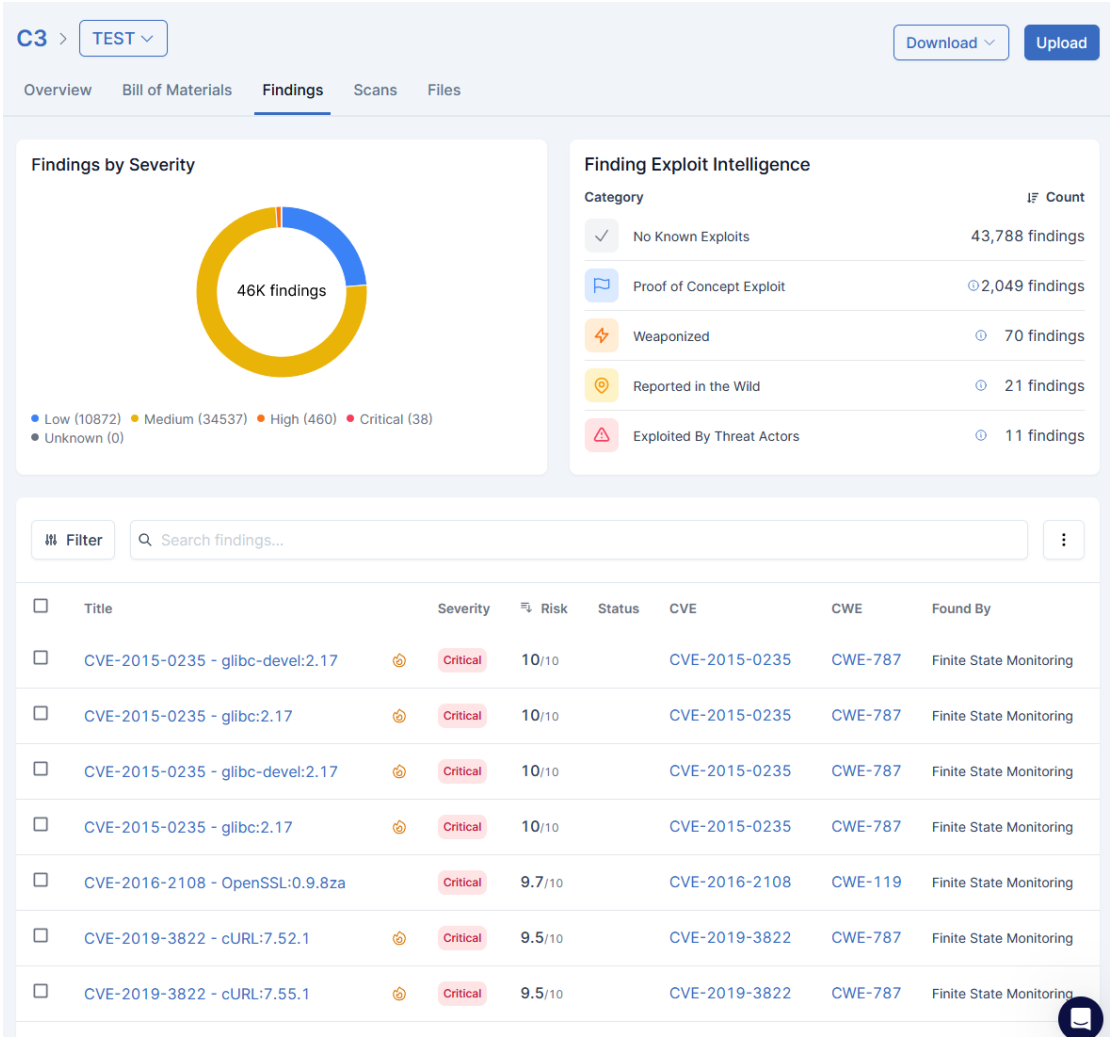


Figure 100: C3 Findings (Finite State Platform)

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

C3_TEST.findings

Figure 101: C3 Findings Categories (Finite State Platform)

A	B	C	D	G	H	I
vulnIdFromTool	riskScore	cvssV3Score	cvssVectorString	affectedComponents	exploitCount	maxExploitMaturity
CVE-2020-1967	7.2	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	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	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	poc
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	poc
CVE-2018-20843	7.4	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	expat: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	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-2019-3822	9.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I	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:	cURL:7.52.1	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:1.1.1k	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	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	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	OpenSSL:1.1.0	2	poc
CVE-2016-6305	7.2	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	OpenSSL:1.1.0	1	poc
CVE-2017-3730	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	OpenSSL:1.1.0	4	poc
CVE-2016-7054	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	OpenSSL:1.1.0	2	poc
CVE-2017-3730	7.4	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	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	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	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	OpenSSL:1.1.0	1	poc
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	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:1.0.2n	1	poc
CVE-2022-0435	7.2	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:	Linux Kernel:4.19.82	2	poc
CVE-2018-16601	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/	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/	FreeRTOS:7.0.0	1	poc
CVE-2018-16526	7.3	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/	FreeRTOS:7.0.0	1	poc
CVE-2018-16526	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-2018-16601	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	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/	FreeRTOS:8.2.3	1	poc
CVE-2019-6974	7.4	8.1	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/	Linux Kernel:4.9.115	6	poc
CVE-2020-14305	7.3	8.1	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/	Linux Kernel:4.9.115	1	poc
CVE-2022-0435	7.2	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:	Linux Kernel:4.9.115	2	poc
CVE-2019-11477	7.5	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	Linux Kernel:4.9.115	1	poc
CVE-2019-11479	7.5	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	Linux Kernel:4.9.115	1	poc
CVE-2019-11478	7.5	7.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I	Linux Kernel:4.9.115	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	glibc:2.18	1	poc
CVE-2014-9984	8.5	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I	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	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/	glibc:2.18	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	glibc:2.18	1	poc
CVE-2014-9402	7.4			glibc:2.18	3	poc
CVE-2014-9402	7.4			glibc:2.18	3	poc
CVE-2014-9984	8.5	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I	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	glibc:2.18	2	poc
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	poc
CVE-2015-7547	8.1	8.1	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C: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	glibc:2.18	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:1.0.2k	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	Linux Kernel:4.19.31	1	poc

C3_TEST.exploit-intel

Figure 102: C3 CVE Exploitability (Finite State Platform)

APPENDIX F: CST SCAN REPORT EXCERPTS FOR SAMPLE C4

Sample C4 Black Duck Scan Report Excerpts

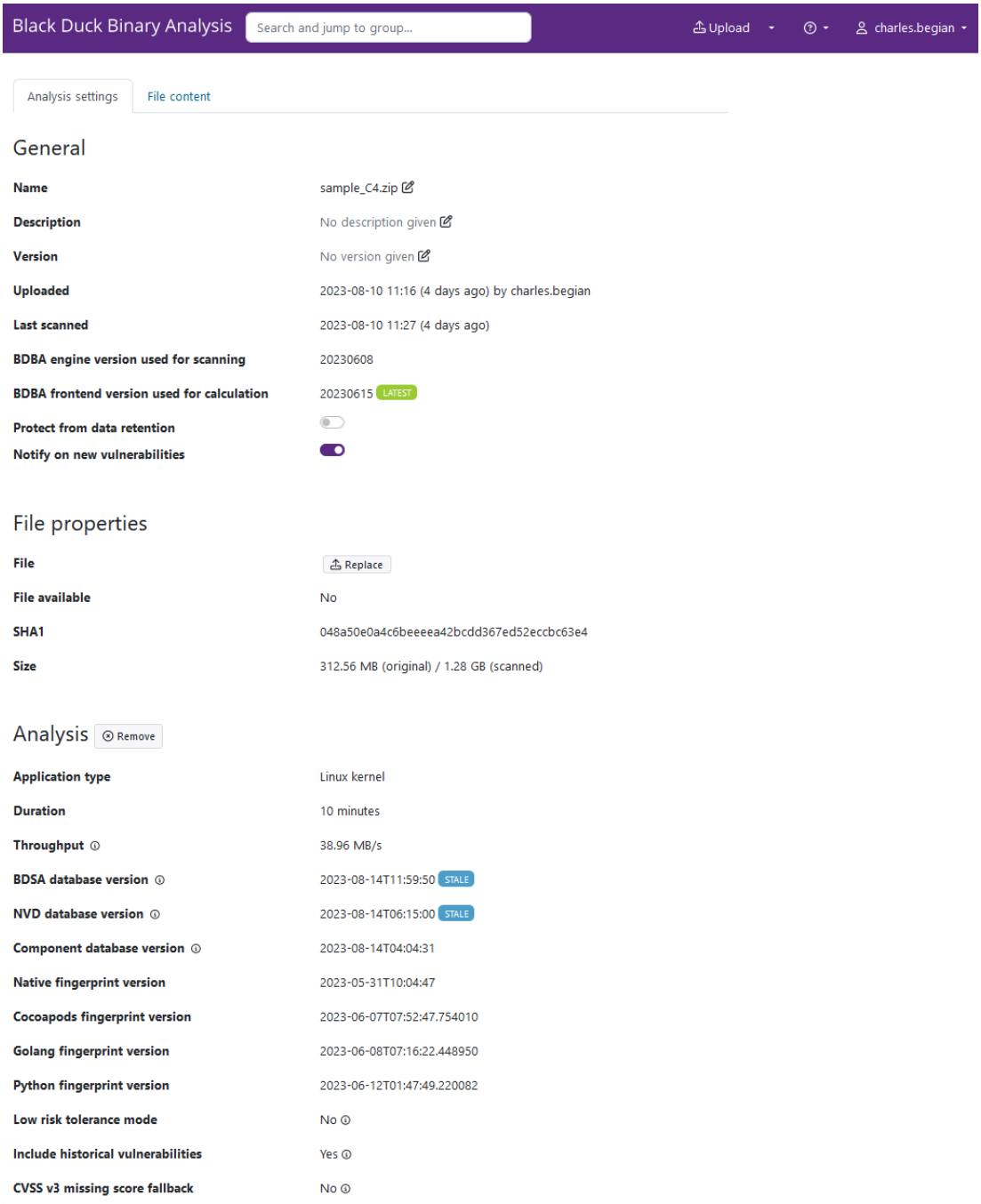
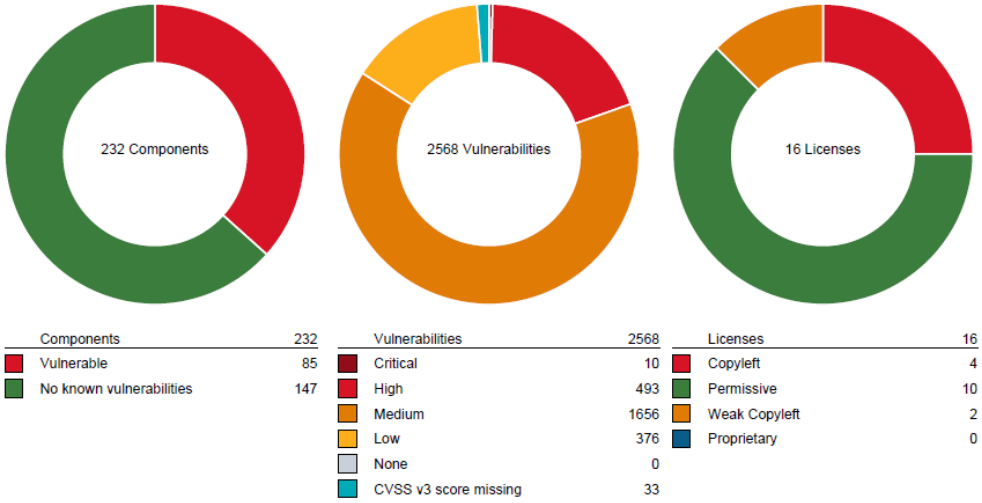


Figure 103: C4 Scan Overview (Black Duck)

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

sample_C4.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY



Components	232
Vulnerable	85
No known vulnerabilities	147

Vulnerabilities	2568
Critical	10
High	493
Medium	1656
Low	376
None	0
CVSS v3 score missing	33

Licenses	16
Copyleft	4
Permissive	10
Weak Copyleft	2
Proprietary	0

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

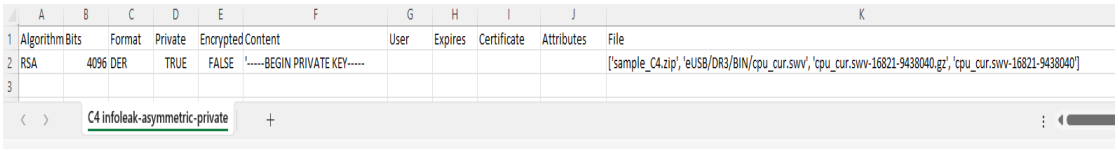
Details

Original filename	
SHA1 checksum	048a50e0a4c6beeeea42bcdd367ed52eccbc63e4
Original file size	312.56 MB

Infoleak

Asymmetric keys:	523
AWS keys:	0
Custom pattern matches:	0
Emails:	2384
HTTP authentication:	0
Image metadata:	0
IP addresses:	2148
JSON web tokens:	0
MAC addresses:	38
OAuth tokens:	0
Passwords:	10
Shell history:	4
URLs:	3238
Twilio keys:	0
Google cloud keys:	0
Facebook access tokens:	0

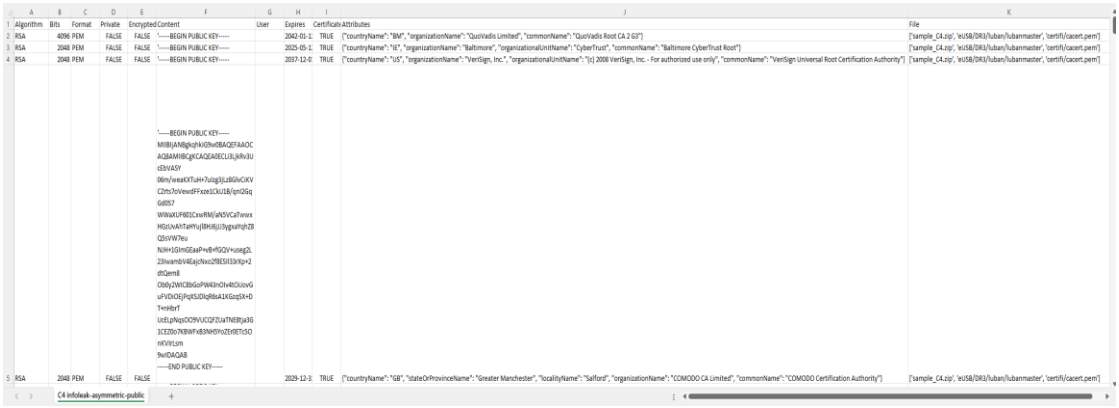
Figure 105: C4 Scan Overview (Black Duck)



Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File
RSA	4096	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']

C4 infoleak-asymmetric-private

Figure 106: C4 Asymmetric keys (Black Duck)



Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File
RSA	4096	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2042-01-1	TRUE	{"countryName": "BM", "organizationName": "QuoVadis Limited", "commonName": "QuoVadis Root CA 2 G3"}	['sample_C4.zip', 'eUSB/DR3/luban/lubanmaster', 'certif/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2025-05-1	TRUE	{"countryName": "IE", "organizationName": "Baltimore", "organizationalUnitName": "CyberTrust", "commonName": "Baltimore CyberTrust Root"}	['sample_C4.zip', 'eUSB/DR3/luban/lubanmaster', 'certif/cacert.pem']
RSA	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', 'eUSB/DR3/luban/lubanmaster', 'certif/cacert.pem']
RSA	2048	PEM	FALSE	FALSE	'-----BEGIN PUBLIC KEY-----		2029-12-3	TRUE	{"countryName": "GB", "stateOrProvinceName": "Greater Manchester", "localityName": "Salford", "organizationName": "COMODO CA Limited", "commonName": "COMODO Certification Authority"}	['sample_C4.zip', 'eUSB/DR3/luban/lubanmaster', 'certif/cacert.pem']

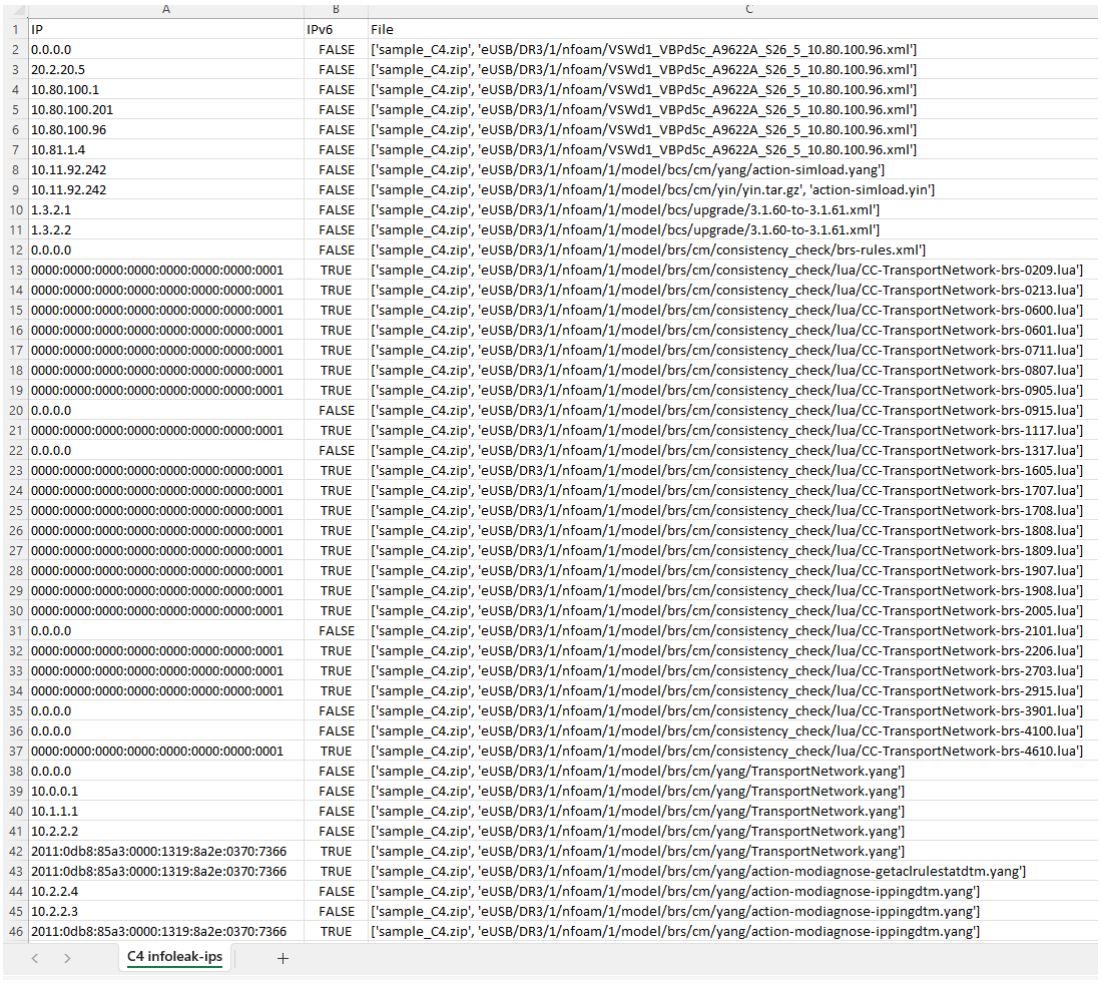
C4 infoleak-asymmetric-public

Figure 107: C4 Symmetric keys (Black Duck)

Email	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
jseward@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
linux-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
jseward@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/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'sbin/curl']	frontec.se
jseward@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
jseward@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
jseward@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
lasse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/lzmadec']	tukaani.org
lasse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/lzmainfo']	tukaani.org
ssh-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
ecdsa-sha2-nistp384-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
lasse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/xzdec']	tukaani.org
lasse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/xzdiff']	tukaani.org
lasse.collin@tukaani.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/bin/xzgrep']	tukaani.org
bkoz@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/c++locale.h']	redhat.com
bkoz@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
bkoz@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
stephen@networkplumber.org	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'usr/include/include/json_writer.h']	networkplumber.org
jiri@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
buytenh@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
jseward@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
steven.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
liw@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
amauryfa@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
solipsis@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
info@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
somebody@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
tarek@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
foo@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
scr@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
foo@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
scr@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
scr@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
0GK500B01D0B8Y@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
W.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
alejandro.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
w.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
perfinion@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
rhallisey@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
jordi@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

C4 infoleak-emails

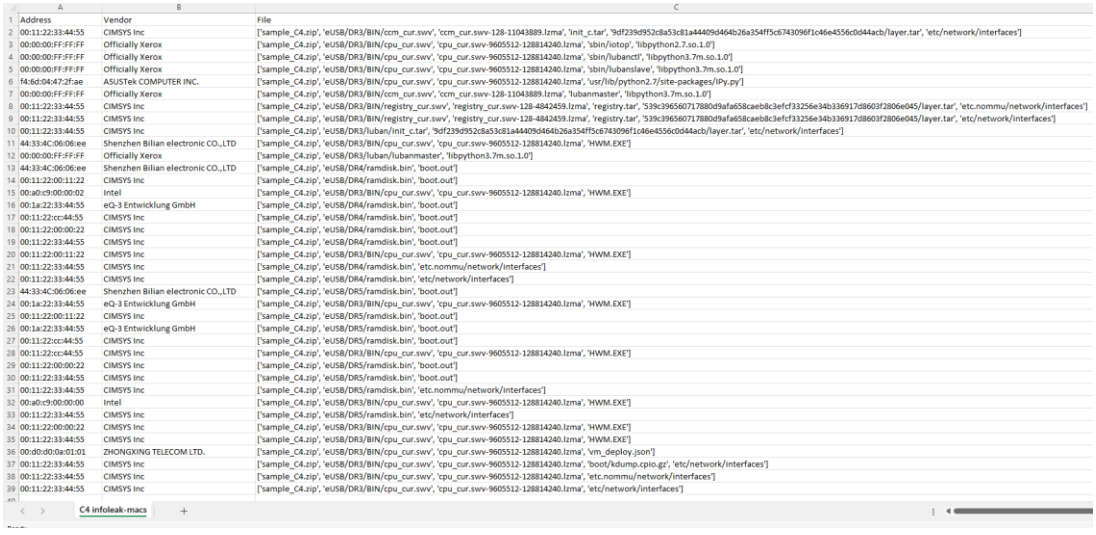
Figure 108: Infoleak email addresses (Black Duck)



	A	B	C
1	IP	IPv6	File
2	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
3	20.2.20.5	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
4	10.80.100.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
5	10.80.100.201	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
6	10.80.100.96	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
7	10.81.1.4	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/VSWd1_VBPd5c_A9622A_S26_5_10.80.100.96.xml']
8	10.11.92.242	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/yang/action-simload.yang']
9	10.11.92.242	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/yin/yin.tar.gz', 'action-simload.yin']
10	1.3.2.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/upgrade/3.1.60-to-3.1.61.xml']
11	1.3.2.2	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/upgrade/3.1.60-to-3.1.61.xml']
12	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/brs-rules.xml']
13	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-0209.lua']
14	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-0213.lua']
15	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-0600.lua']
16	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-0601.lua']
17	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']
18	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']
19	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']
20	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-0915.lua']
21	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-1117.lua']
22	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-1317.lua']
23	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-1605.lua']
24	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-1707.lua']
25	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']
26	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-1808.lua']
27	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']
28	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-1907.lua']
29	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-1908.lua']
30	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']
31	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-2101.lua']
32	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-2206.lua']
33	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-2703.lua']
34	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-2915.lua']
35	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-3901.lua']
36	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/consistency_check/lua/CC-TransportNetwork-brs-4100.lua']
37	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-4610.lua']
38	0.0.0.0	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
39	10.0.0.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
40	10.1.1.1	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
41	10.2.2.2	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
42	2011:0db8:85a3:0000:1319:8a2e:0370:7366	TRUE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/TransportNetwork.yang']
43	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']
44	10.2.2.4	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/action-modiagnose-ippingdtm.yang']
45	10.2.2.3	FALSE	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/brs/cm/yang/action-modiagnose-ippingdtm.yang']
46	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']

C4 infoleak-ips

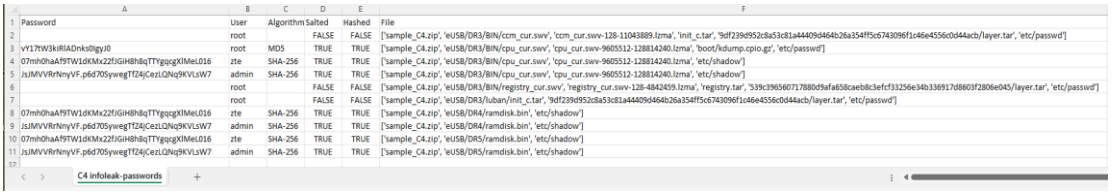
Figure 109: C4 Infoleak IP addresses (Black Duck)



	A	B	C
1	Address	Vendor	File
2	00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/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', 'eUSB/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', 'eUSB/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', 'eUSB/DR3/BIN/ccm_cur.swv', 'ccm_cur.swv-128-11043889.lzma', '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-128-4842459.lzma', 'registry.tar', '539c396560717880d9afa658caeb8c3efcf33256e34b336917d8603f2806e045/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/init_c.tar', '9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/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', 'eUSB/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', 'eUSB/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', 'eUSB/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', 'eUSB/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', 'eUSB/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', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'etc.nommu/network/interfaces']
39	00:11:22:33:44:55	CIMSYS Inc	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'etc/network/interfaces']

C4 infoleak-macs

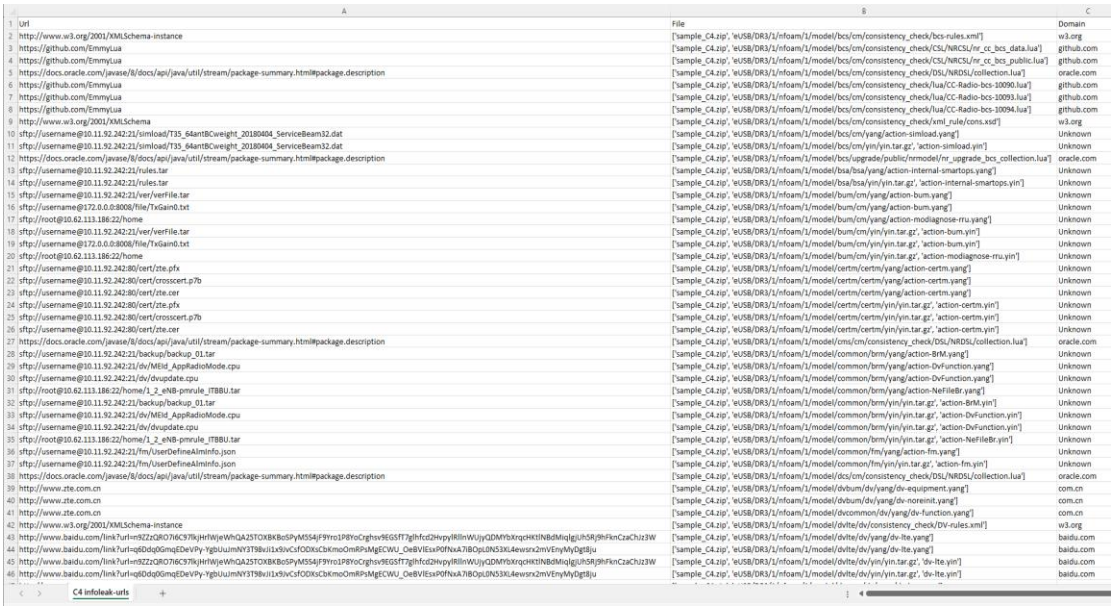
Figure 110: C4 Infoleak MAC addresses (Black Duck)



	A	B	C	D	E	F
1	Password	User	Algorithm	Salted	Hashed	File
2		root		FALSE	FALSE	['sample_C4.zip', 'eUSB/DR3/BIN/ccm_cur.swv', 'ccm_cur.swv-128-11043889.lzma', 'init_c.tar', '9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/layer.tar', 'etc/passwd']
3	vY17fW3kiRlADnksIligyI0	root	MD5	TRUE	TRUE	['sample_C4.zip', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'boot/kdump.cpio.gz', 'etc/passwd']
4	07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	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', 'eUSB/DR3/BIN/cpu_cur.swv', 'cpu_cur.swv-9605512-128814240.lzma', 'etc/shadow']
6		root		FALSE	FALSE	['sample_C4.zip', 'eUSB/DR3/BIN/registry_cur.swv', 'registry_cur.swv-128-4842459.lzma', 'registry.tar', '339c396560717880d9afa658caeb8c3efcf33256e34b336917d8603f2806e045/layer.tar', 'etc/passwd']
7		root		FALSE	FALSE	['sample_C4.zip', 'eUSB/DR3/luban/init_c.tar', '9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/layer.tar', 'etc/passwd']
8	07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	zte	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'etc/shadow']
9	JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUSB/DR4/ramdisk.bin', 'etc/shadow']
10	07mh0haAf9TW1dKMx22fJGiH8h8qTTYgqcgXlMeL016	zte	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'etc/shadow']
11	JsJMVVRrNnyVF.p6d70SywegTfZ4jCezLQNq9KVLsW7	admin	SHA-256	TRUE	TRUE	['sample_C4.zip', 'eUSB/DR5/ramdisk.bin', 'etc/shadow']
12						

C4 infoleak-passwords

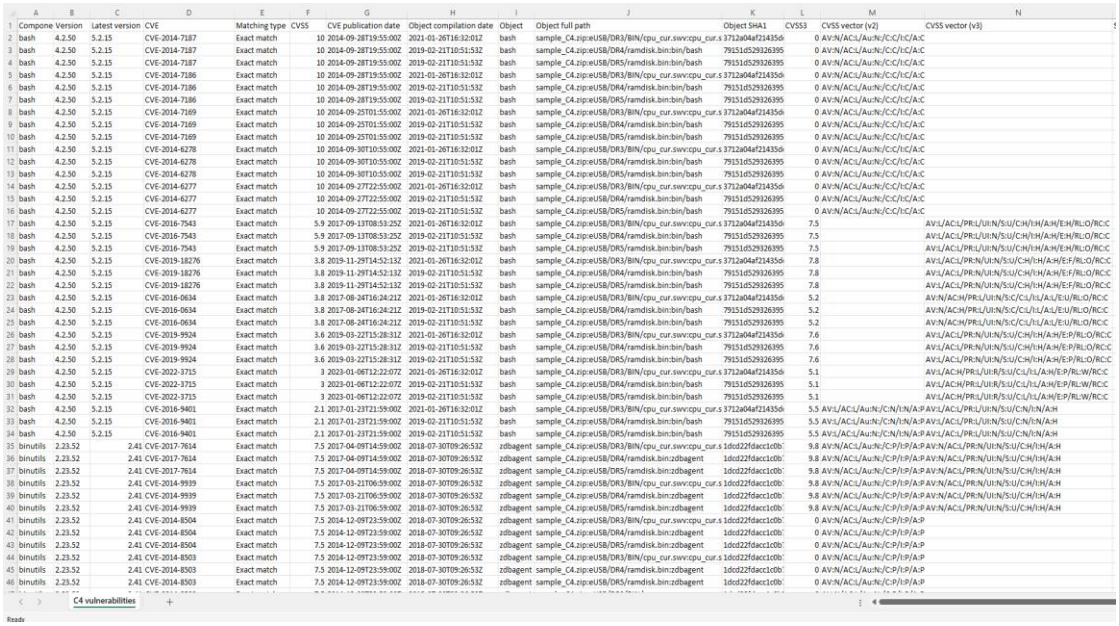
Figure 111: C4 Infoleak passwords (Black Duck)



	A	B	C
1	Url	File	Domain
2	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
3	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.com
4	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
5	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
6	https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/lua/CC-Radio-bcs-10090.lua']	github.com
7	https://github.com/EmmyLua	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/lua/CC-Radio-bcs-10093.lua']	github.com
8	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
9	http://www.w3.org/2001/XMLSchema	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/consistency_check/xml_rule/cons.xsd']	w3.org
10	sftp://username@10.11.92.242:21/simload/T35_64antBCweight_20180404_ServiceBeam32.dat	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bcs/cm/yang/action-simload.yang']	Unknown
11	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
12	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
13	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
14	sftp://username@10.11.92.242:21/rules.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bsa/bsa/yin/yin.tar.gz', 'action-internal-smartops.yin']	Unknown
15	sftp://username@10.11.92.242:21/ver/verFile.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yang/action-bum.yang']	Unknown
16	sftp://username@172.0.0.0:8008/file/TxGain0.txt	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yang/action-bum.yang']	Unknown
17	sftp://root@10.62.113.186:22/home	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yang/action-modiagnose-rru.yang']	Unknown
18	sftp://username@10.11.92.242:21/ver/verFile.tar	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yin/yin.tar.gz', 'action-bum.yin']	Unknown
19	sftp://username@172.0.0.0:8008/file/TxGain0.txt	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yin/yin.tar.gz', 'action-bum.yin']	Unknown
20	sftp://root@10.62.113.186:22/home	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/bum/cm/yin/yin.tar.gz', 'action-modiagnose-rru.yin']	Unknown
21	sftp://username@10.11.92.242:80/cert/zte.pfx	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yang/action-certm.yang']	Unknown
22	sftp://username@10.11.92.242:80/cert/crosscert.p7b	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yang/action-certm.yang']	Unknown
23	sftp://username@10.11.92.242:80/cert/zte.cer	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/certm/certm/yang/action-certm.yang']	Unknown
24	sftp://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
25	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
26	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
27	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.com
28	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
29	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
30	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
31	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
32	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
33	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
34	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
35	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/yin/yin.tar.gz', 'action-NeFileBr.yin']	Unknown
36	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
37	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
38	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
39	http://www.zte.com.cn	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvbum/dv/yang/dv-equipment.yang']	com.cn
40	http://www.zte.com.cn	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvbum/dv/yang/dv-noreinit.yang']	com.cn
41	http://www.zte.com.cn	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvcommon/dv/yang/dv-function.yang']	com.cn
42	http://www.w3.org/2001/XMLSchema-instance	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvlte/dv/consistency_check/DV-rules.xml']	w3.org
43	http://www.baidu.com/link?url=n9ZZzQRO7l6C97lkjHrlWjeWhQA2STOXBKBoSPyM554jF9Yro1P8YoCrghsv9EG5fT7glhfcd2HvpyIRlInWUjyQDMYbXrqcHKtlNBdMIqIgUh5R/9hFkmCzaChJz3W	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvlte/dv/yang/dv-lte.yang']	baidu.com
44	http://www.baidu.com/link?url=q6Ddq0GmqEDeVPy-YgbUuJmNY3T9BwJi1x9vCsfODKsCbKmoOmRPsMgECWU_OeBVIEsxP0fNxA7iBOpL0N53XL4ewsrx2mVEnyMyDgt8ju	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvlte/dv/yang/dv-lte.yang']	baidu.com
45	http://www.baidu.com/link?url=n9ZZzQRO7l6C97lkjHrlWjeWhQA2STOXBKBoSPyM554jF9Yro1P8YoCrghsv9EG5fT7glhfcd2HvpyIRlInWUjyQDMYbXrqcHKtlNBdMIqIgUh5R/9hFkmCzaChJz3W	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvlte/dv/yin/yin.tar.gz', 'dv-lte.yin']	baidu.com
46	http://www.baidu.com/link?url=q6Ddq0GmqEDeVPy-YgbUuJmNY3T9BwJi1x9vCsfODKsCbKmoOmRPsMgECWU_OeBVIEsxP0fNxA7iBOpL0N53XL4ewsrx2mVEnyMyDgt8ju	['sample_C4.zip', 'eUSB/DR3/1/nfoam/1/model/dvlte/dv/yin/yin.tar.gz', 'dv-lte.yin']	baidu.com

C4 infoleak-urls

Figure 112: C4 Infoleak URLs (Black Duck)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Compone	Version	Latest version	CVE	Matching type	CVSS	CVE publication date	Object compilation date	Object	Object full path	Object SHA1	CVSS3	CVSS vector (v2)	CVSS vector (v3)
2	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_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
3	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_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
4	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_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
5	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	3712a04af214350	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
6	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_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
7	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_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
8	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	3712a04af214350	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
9	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/DR4/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
10	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	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
11	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	3712a04af214350	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
12	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_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
13	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_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
14	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_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
15	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_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
16	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_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	0	AV:N/AC:L/Au:N/C:C/I:C/A:C	
17	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_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	7.5		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
18	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_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	7.5		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
19	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_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	7.5		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
20	bash	4.2.50	5.2.15	CVE-2019-18276	Exact match	3.8	2019-11-29T14:52:13Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	7.8		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
21	bash	4.2.50	5.2.15	CVE-2019-18276	Exact match	3.8	2019-11-29T14:52:13Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	7.8		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
22	bash	4.2.50	5.2.15	CVE-2019-18276	Exact match	3.8	2019-11-29T14:52:13Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	7.8		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
23	bash	4.2.50	5.2.15	CVE-2016-0634	Exact match	3.8	2017-08-24T16:24:21Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	5.2		AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C
24	bash	4.2.50	5.2.15	CVE-2016-0634	Exact match	3.8	2017-08-24T16:24:21Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	5.2		AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C
25	bash	4.2.50	5.2.15	CVE-2016-0634	Exact match	3.8	2017-08-24T16:24:21Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	5.2		AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L/E:U/RL:O/RC:C
26	bash	4.2.50	5.2.15	CVE-2019-9924	Exact match	3.6	2019-03-22T15:28:31Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	7.6		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
27	bash	4.2.50	5.2.15	CVE-2019-9924	Exact match	3.6	2019-03-22T15:28:31Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	7.6		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
28	bash	4.2.50	5.2.15	CVE-2019-9924	Exact match	3.6	2019-03-22T15:28:31Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	7.6		AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
29	bash	4.2.50	5.2.15	CVE-2022-3715	Exact match	3	2023-01-06T12:22:07Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	5.1		AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:W/RC:C
30	bash	4.2.50	5.2.15	CVE-2022-3715	Exact match	3	2023-01-06T12:22:07Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	5.1		AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:W/RC:C
31	bash	4.2.50	5.2.15	CVE-2022-3715	Exact match	3	2023-01-06T12:22:07Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	5.1		AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:W/RC:C
32	bash	4.2.50	5.2.15	CVE-2016-9401	Exact match	2.1	2017-01-23T21:59:00Z	2021-01-26T16:32:01Z	bash	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	3712a04af214350	5.5	AV:L/AC:L/Au:N/C:N/I:N/A:P	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
33	bash	4.2.50	5.2.15	CVE-2016-9401	Exact match	2.1	2017-01-23T21:59:00Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR4/ramdisk.bin:bin/bash	79151d529326395	5.5	AV:L/AC:L/Au:N/C:N/I:N/A:P	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
34	bash	4.2.50	5.2.15	CVE-2016-9401	Exact match	2.1	2017-01-23T21:59:00Z	2019-02-21T10:51:53Z	bash	sample_C4.zip:eUSB/DR5/ramdisk.bin:bin/bash	79151d529326395	5.5	AV:L/AC:L/Au:N/C:N/I:N/A:P	AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
35	binutils	2.23.52	2.41	CVE-2017-7614	Exact match	7.5	2017-04-09T14:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	1dcd22fdacc1c0b	9.8	AV:N/AC:L/Au:N/C:P/I:P/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
36	binutils	2.23.52	2.41	CVE-2017-7614	Exact match	7.5	2017-04-09T14:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR4/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	9.8	AV:N/AC:L/Au:N/C:P/I:P/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
37	binutils	2.23.52	2.41	CVE-2017-7614	Exact match	7.5	2017-04-09T14:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR5/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	9.8	AV:N/AC:L/Au:N/C:P/I:P/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
38	binutils	2.23.52	2.41	CVE-2014-9939	Exact match	7.5	2017-03-21T06:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	1dcd22fdacc1c0b	9.8	AV:N/AC:L/Au:N/C:P/I:P/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
39	binutils	2.23.52	2.41	CVE-2014-9939	Exact match	7.5	2017-03-21T06:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR4/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	9.8	AV:N/AC:L/Au:N/C:P/I:P/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
40	binutils	2.23.52	2.41	CVE-2014-9939	Exact match	7.5	2017-03-21T06:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR5/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	9.8	AV:N/AC:L/Au:N/C:P/I:P/A:P	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
41	binutils	2.23.52	2.41	CVE-2014-8504	Exact match	7.5	2014-12-09T23:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	1dcd22fdacc1c0b	0	AV:N/AC:L/Au:N/C:P/I:P/A:P	
42	binutils	2.23.52	2.41	CVE-2014-8504	Exact match	7.5	2014-12-09T23:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR4/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	0	AV:N/AC:L/Au:N/C:P/I:P/A:P	
43	binutils	2.23.52	2.41	CVE-2014-8504	Exact match	7.5	2014-12-09T23:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR5/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	0	AV:N/AC:L/Au:N/C:P/I:P/A:P	
44	binutils	2.23.52	2.41	CVE-2014-8503	Exact match	7.5	2014-12-09T23:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR3/BIN/cpu_cur.swv:cpu_cur.s	1dcd22fdacc1c0b	0	AV:N/AC:L/Au:N/C:P/I:P/A:P	
45	binutils	2.23.52	2.41	CVE-2014-8503	Exact match	7.5	2014-12-09T23:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR4/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	0	AV:N/AC:L/Au:N/C:P/I:P/A:P	
46	binutils	2.23.52	2.41	CVE-2014-8503	Exact match	7.5	2014-12-09T23:59:00Z	2018-07-30T09:26:53Z	zdbagent	sample_C4.zip:eUSB/DR5/ramdisk.bin:zdbagent	1dcd22fdacc1c0b	0	AV:N/AC:L/Au:N/C:P/I:P/A:P	

C4 vulnerabilities

Ready

Figure 113: C4 CVEs (Black Duck)

Sample C4 Code Sentry Scan Report Excerpts

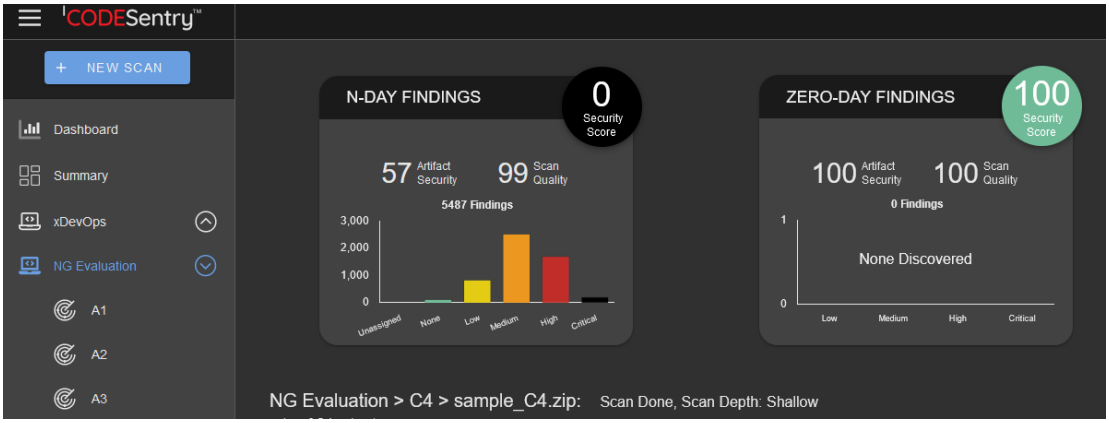


Figure 114: C4 Scan Overview (Code Sentry)

GRAMMATECH CODESentry

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/9df239d952c8a53c81a44409d464b26a354ff5c6743096f1c46e4556c0d44acb/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

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

GRAMMATECH

CODESentry

N-Day Findings

Findings for sample_C4.zip

Scan Depth: **Shallow**
MD5: **cb599c8543567aed45b2eb8f715aabce**
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: Unassigned: 0 None: 26 Low: 267 Medium: 813 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...

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

GRAMMATECH CODESentry

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")	-

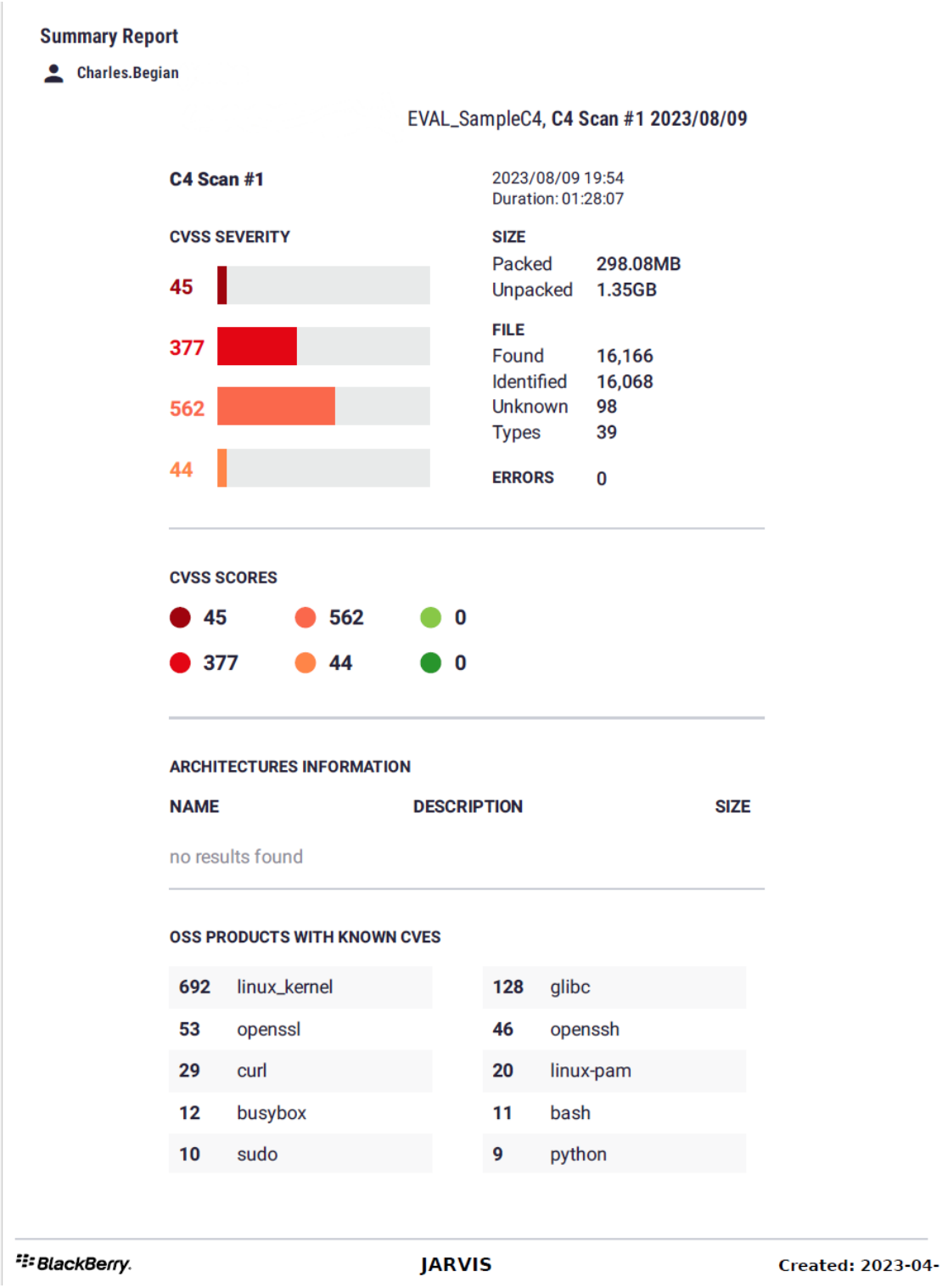
All Other CWE Findings (Excluding Top 25 CWEs)

Severity	Score	CWE ID	Name	Instances

None

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

Sample C4 Jarvis Scan Report Excerpts



Summary Report

Charles.Begian

EVAL_SampleC4, **C4 Scan #1 2023/08/09**

C4 Scan #1

2023/08/09 19:54
Duration: 01:28:07

CVSS SEVERITY

45	
377	
562	
44	

SIZE

Packed	298.08MB
Unpacked	1.35GB

FILE

Found	16,166
Identified	16,068
Unknown	98
Types	39

ERRORS 0

CVSS SCORES

45	562	0
377	44	0

ARCHITECTURES INFORMATION

NAME	DESCRIPTION	SIZE

no results found

OSS PRODUCTS WITH KNOWN CVES

692	linux_kernel	128	glibc
53	openssl	46	openssh
29	curl	20	linux-pam
12	busybox	11	bash
10	sudo	9	python

BlackBerry. JARVIS Created: 2023-04-

Figure 118: C4 Scan Overview (Jarvis)

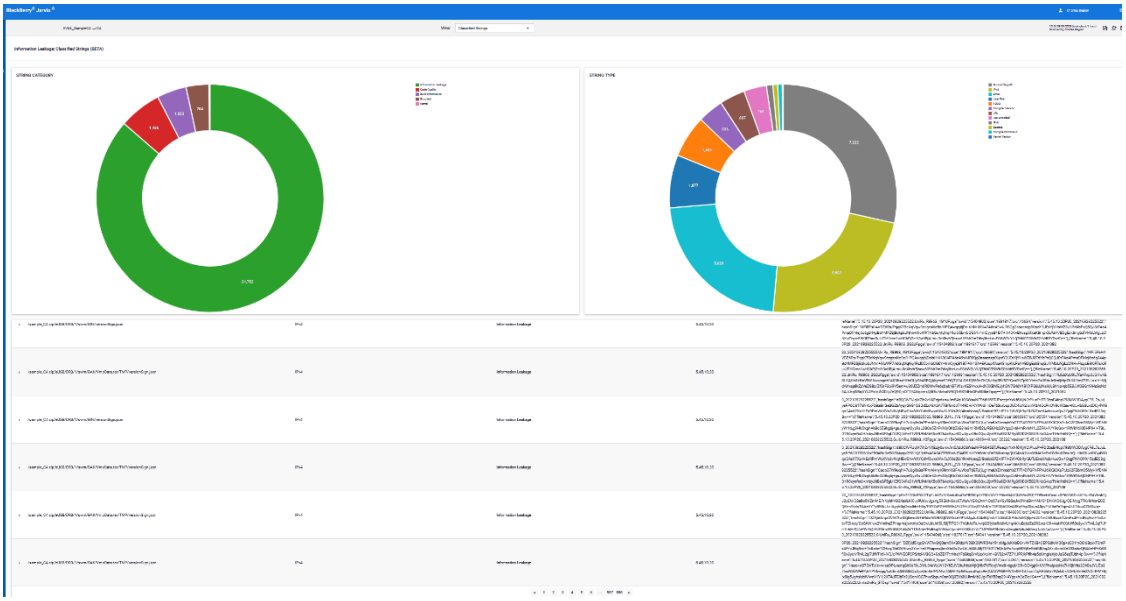


Figure 119: C4 Information leakage (Jarvis)

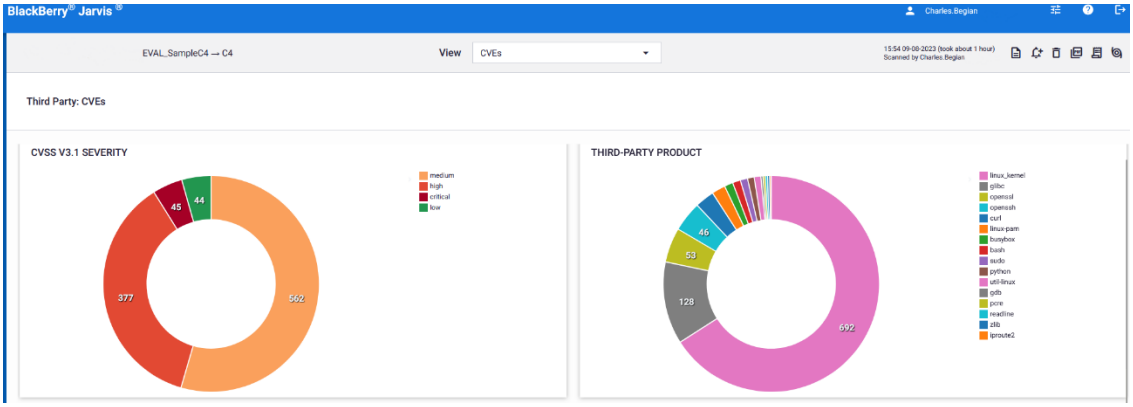


Figure 120: CVSS Severity Report (Jarvis)

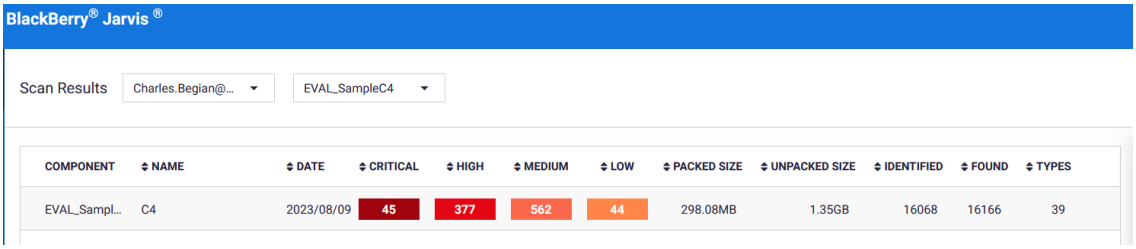


Figure 121: C4 CVE Summary by Severity (Jarvis)

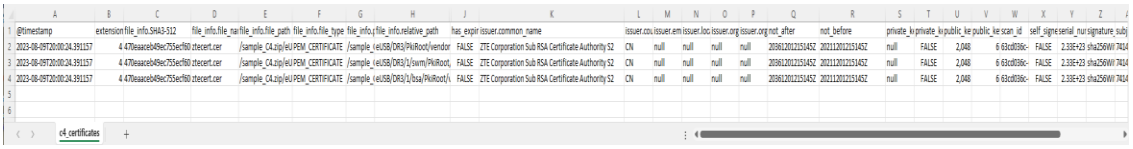


Figure 122: C4 Certificates Report (Jarvis)

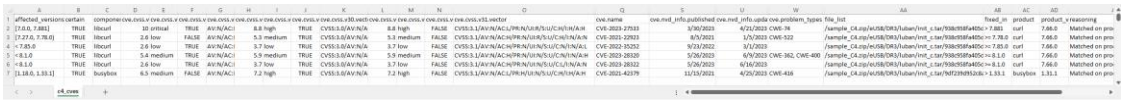


Figure 123: C4 CVEs (Jarvis)

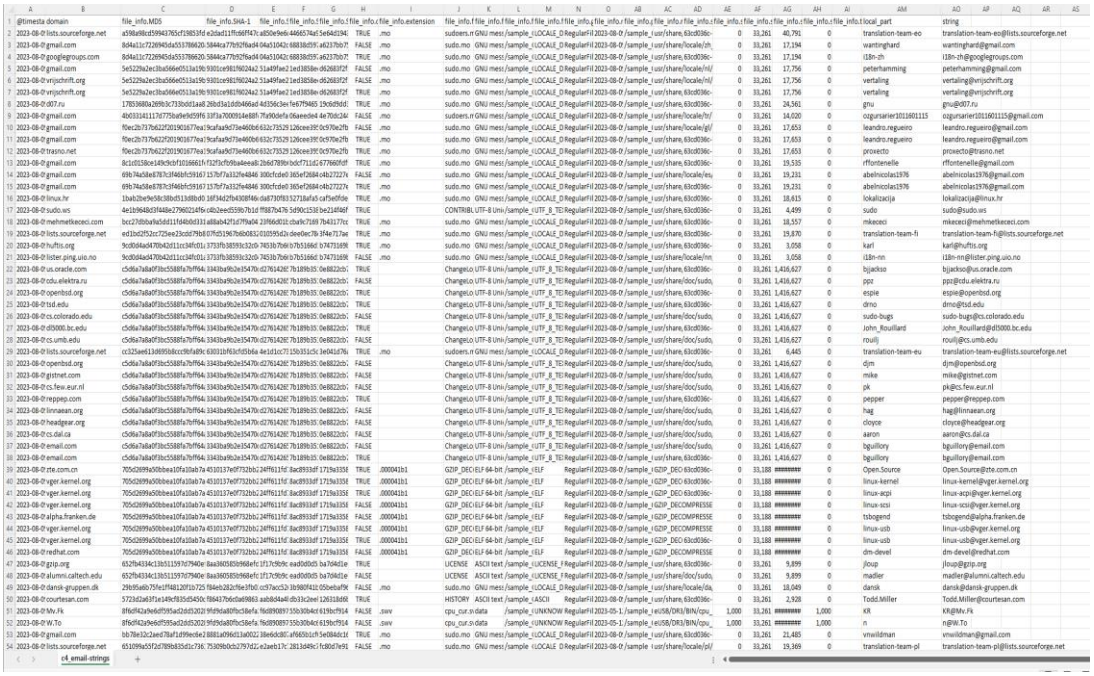


Figure 124: C4 email addresses (Jarvis)

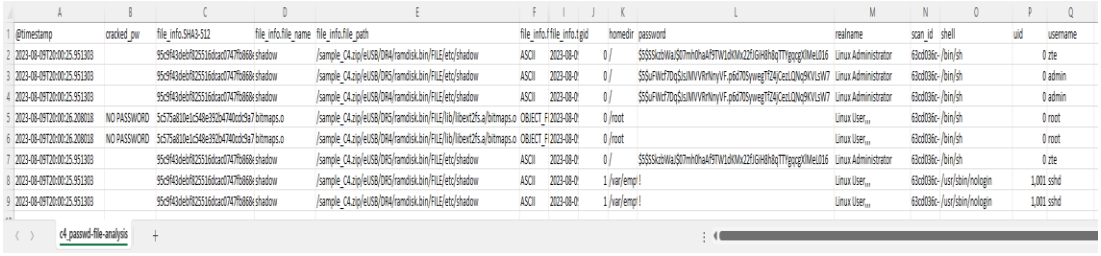


Figure 125: C4 Password File Analysis (Jarvis)

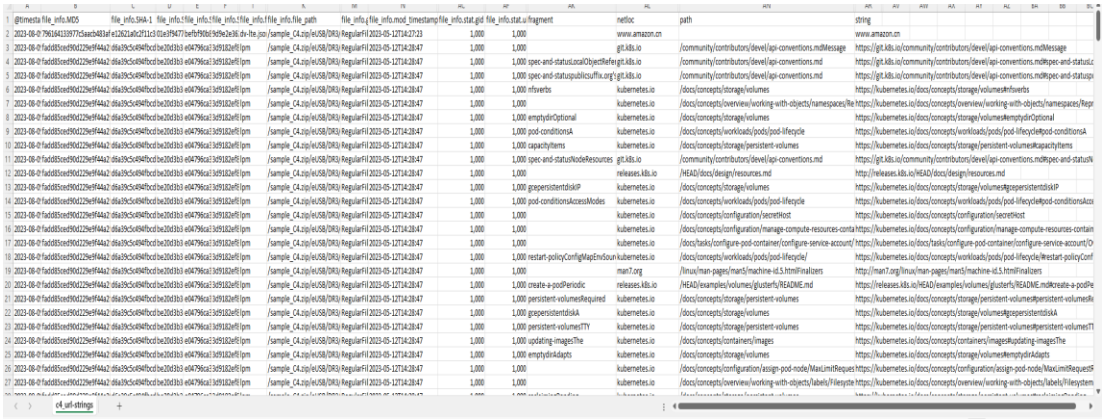


Figure 126: C4 Infoleak URL Report (Jarvis)

Sample C4 Finite State Platform Scan Report Excerpts

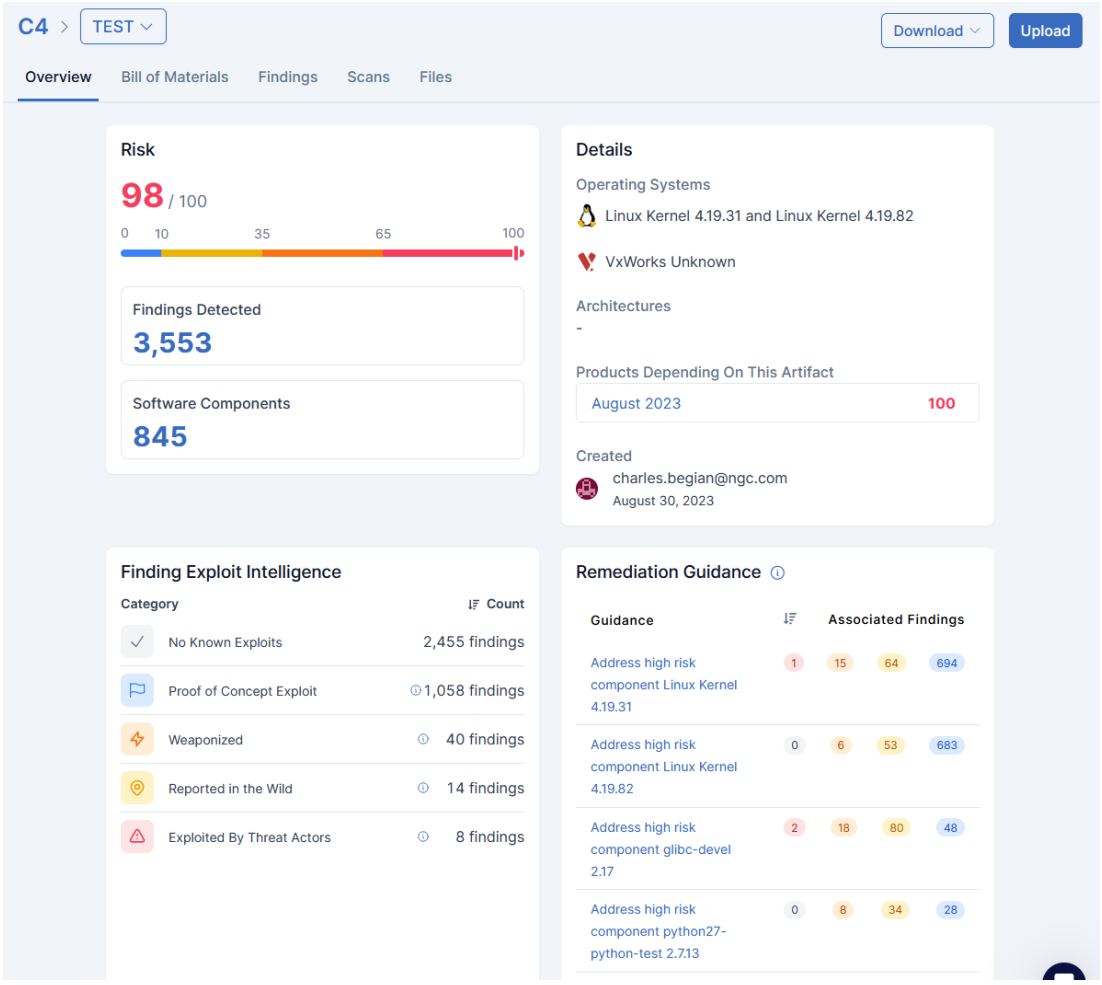


Figure 127: C4 Scan Overview (Finite State Platform)

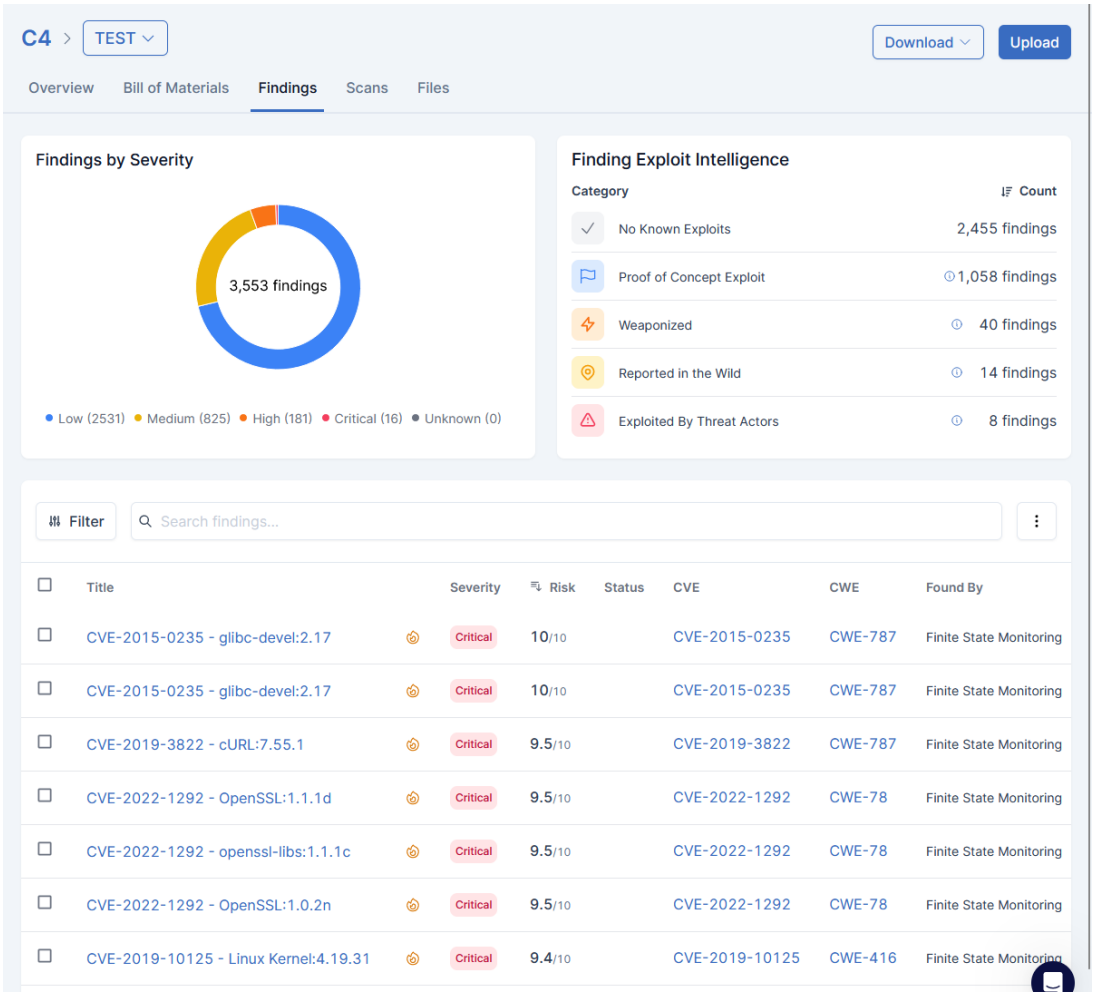


Figure 128: C4 Findings (Finite State Platform)

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)

A	B	C	D	G	H	I
vulnIdFromTool	riskScore	cvssV3Score	cvssVectorString	affectedComponents	exploitCount	maxExploitMaturity
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
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	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:4.19.31	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	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:4.19.31	2	poc
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-2016-7054	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	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-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-2016-8610	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-2016-6305	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-2016-7054	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	poc
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-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	libexpat1-dev:2.2.0-2+deb9u3	1	poc
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	libexpat1-dev:2.2.0-2+deb9u3	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:H/A:H	libexpat1-dev:2.2.0-2+deb9u3	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-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-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-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:2.2.0	1	poc
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	expat:2.2.0	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:H/A:H	expat:2.2.0	1	poc
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	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-2023-38408	8.9	9.8	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	5	weaponized
CVE-2023-38408	8.9	9.8	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	5	weaponized
CVE-2018-15514	8.4	8.8	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	docker-client:1.13.1	1	poc
CVE-2018-15514	8.4	8.8	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	docker-client:1.13.1	1	poc
CVE-2021-3156	7.8	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	67	weaponized
CVE-2019-14287	7.7	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	sudo-devel:1.8.22	6	weaponized
CVE-2018-1000802	7.8	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	python27-python:2.7.13	2	poc
CVE-2018-1000802	7.8	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	python27-python:2.7.13	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-libs:1.1.1c	1	poc
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-util:3.16.2.3	1	poc
CVE-2021-3156	7.8	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	67	weaponized
CVE-2019-14287	7.7	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	sudo:1.8.22	6	weaponized
CVE-2019-19844	9.3	9.8	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	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	libexpat:2.2.0-1	1	poc
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	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	libexpat:2.2.0-1	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-devel:2.17	1	poc
CVE-2015-0235	10			glibc-devel:2.17	29	weaponized
CVE-2014-9402	7.4			glibc-devel:2.17	3	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-devel:2.17	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-devel:2.17	2	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-devel:2.17	1	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-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-intel

Figure 130: C4 CVE Exploitability (Finite State Platform)

APPENDIX G: CST SCAN REPORT EXCERPTS FOR SAMPLE C5

Sample C5 Black Duck Scan Report Excerpts

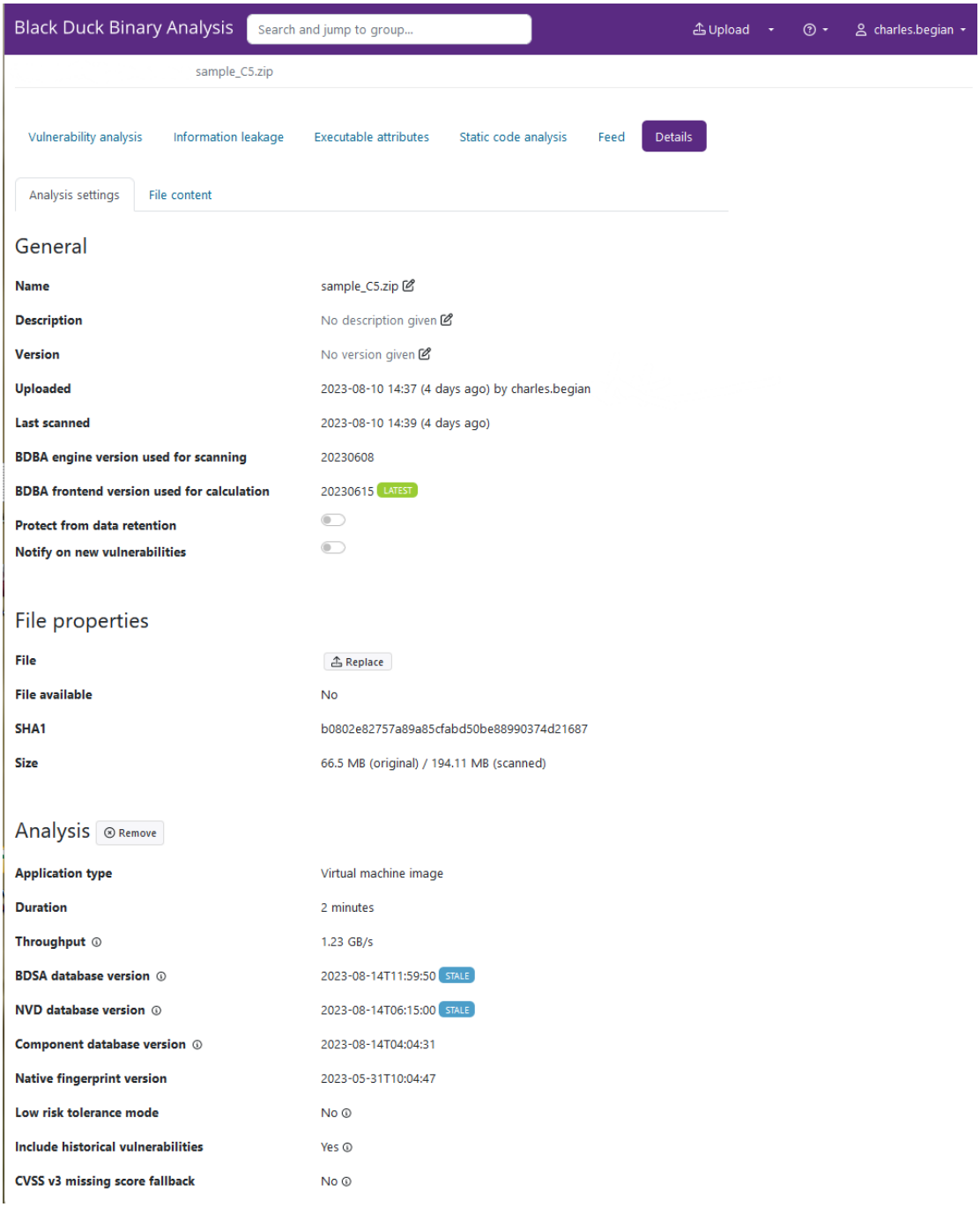
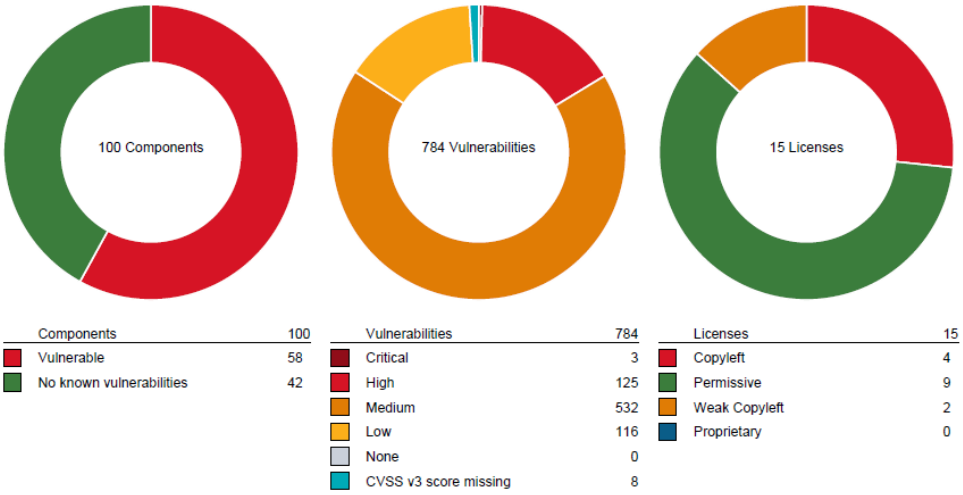


Figure 131: C5 Scan Overview (Black Duck)

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

sample_C5.zip

Vulnerability analysis verdict: VULNS / Information leakage: VERIFY



Components	100
Vulnerable	58
No known vulnerabilities	42

Vulnerabilities	784
Critical	3
High	125
Medium	532
Low	116
None	0
CVSS v3 score missing	8

Licenses	15
Copyleft	4
Permissive	9
Weak Copyleft	2
Proprietary	0

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

Details

Original filename	
SHA1 checksum	b0802e82757a89a85cfabd50be88990374d21687
Original file size	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

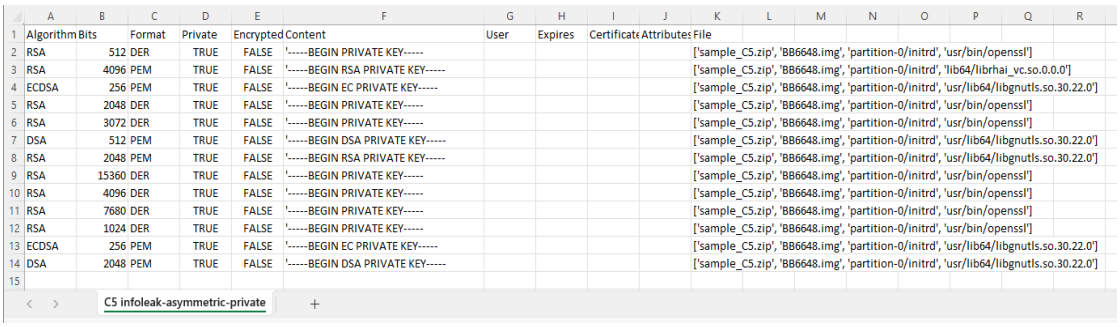
This result is a product of an automatic analysis and may contain errors or omissions.

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)



Algorithm	Bits	Format	Private	Encrypted	Content	User	Expires	Certificate	Attributes	File
RSA	512	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
RSA	4096	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'lib64/librhai_vc.so.0.0.0']
ECDSA	256	PEM	TRUE	FALSE	'-----BEGIN EC PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libgnutls.so.30.22.0']
RSA	2048	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
RSA	3072	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
DSA	512	PEM	TRUE	FALSE	'-----BEGIN DSA PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libgnutls.so.30.22.0']
RSA	2048	PEM	TRUE	FALSE	'-----BEGIN RSA PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libgnutls.so.30.22.0']
RSA	15360	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
RSA	4096	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
RSA	7680	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
RSA	1024	DER	TRUE	FALSE	'-----BEGIN PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/openssl']
ECDSA	256	PEM	TRUE	FALSE	'-----BEGIN EC PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libgnutls.so.30.22.0']
DSA	2048	PEM	TRUE	FALSE	'-----BEGIN DSA PRIVATE KEY-----					['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libgnutls.so.30.22.0']

C5 infoleak-asymmetric-private

Figure 134: C5 Asymmetric keys (Black Duck)

C5 infoleak-asymmetric-public

Figure 135: C5 Symmetric keys (Black Duck)

Email	File	Domain
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
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
ssh-ed25519-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
umac-128-etm@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
forwarded-streamlocal@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
ecdsa-sha2-nistp384-cert-v01@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
cancel-streamlocal-forward@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/ssh.openssh']	openssh.com
procps@freelists.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/bin/top.procps']	freelists.org
jseward@bzip.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/lib64/libbz2.so.1.0.6']	bzip.org
tun@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
hostkeys-00@openssh.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
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_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/sbin/sshd']	openssh.com
SIG@openssh.com	['sample_C5.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', 'bin/cpio.cpio']	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
aschorr@telemetry-investments.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/awk/have_mpfr.awk']	telemetry-investments.com
aschorr@telemetry-investments.com	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'usr/share/awk/inplace.awk']	telemetry-investments.com
ajt@debian.org	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/services']	debian.org
hakan@erix.ericsson.se	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/otp/lib/tftp-1.0.1/src/tftp.erl']	ericsson.se

C5 infoleak-emails

Figure 136: C5 Infoleak email addresses (Black Duck)

	A	B	C
1	IP	IPv6	File
2	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
3	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
4	192.168.0.254	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
5	192.168.0.20	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/busybox.nosuid']
6	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/ping.iputils']
7	10.18.44.13	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/build-info']
8	10.18.44.13	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/build-info.sh']
9	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/hosts']
10	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
11	255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
12	192.5.5.213	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
13	192.33.137.200	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
14	192.33.137.209	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
15	192.33.137.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
16	192.33.137.250	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/dhcp/dhclient.conf']
17	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
18	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
19	169.254.1.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
20	169.254.1.2	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
21	169.254.1.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/pghd/lmt.sh']
22	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
23	127.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
24	192.168.200.9	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
25	192.168.200.4	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
26	192.168.200.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
27	192.168.201.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
28	2001:4ca0:0:101::1	TRUE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
29	2001:4ca0:0:101:0:0:0:1	TRUE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/security/access.conf']
30	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/ssh/sshd_config']
31	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/ssh/sshd_config_readonly']
32	1.2.3.4	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'etc/ssl/openssl.cnf']
33	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'lib64/libresolv-2.28.so']
34	10.11.12.13	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/autointegrate']
35	10.68.200.11	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/autointegrate']
36	141.1.2.3	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/autointegrate']
37	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/bin/nl_util']
38	10.1.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/etc/ipsec.conf']
39	10.2.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/etc/ipsec.conf']
40	192.168.0.2	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/etc/ipsec.conf']
41	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/lib64/ipsec/libcharon.so.0.0.0']
42	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/lib64/ipsec/libstrongswan.so.0.0.0']
43	0.0.0.0	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'nl/strongswan/lib64/ipsec/plugins/libstrongswan-stroke.so']
44	255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/arp.net-tools']
45	FF02::1:2	TRUE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/dhclient']
46	255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/dhclient-script']
47	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/epghd']
48	127.0.0.1	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/htmd']
49	255.255.255.255	FALSE	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'sbin/ifcfg']

C5 infoleak-ips

Figure 137: C5 Infoleak IP addresses (Black Duck)

	A	B	C
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 infoleak-macs

Figure 138: C5 Infoleak MAC addresses (Black Duck)

	A	B	C	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 infoleak-passwords

Figure 139: C5 Infoleak passwords (Black Duck)

	A	B	C
1	Url	File	Domain
2	http://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash']	gnu.org
3	http://www.gnu.org/software/bash	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash']	gnu.org
4	http://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/bash.bash']	gnu.org
5	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils']	gnu.org
6	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils']	gnu.org
7	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils']	translationproject.org
8	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cat.coreutils']	gnu.org
9	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils']	gnu.org
10	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils']	gnu.org
11	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils']	translationproject.org
12	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chgrp.coreutils']	gnu.org
13	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils']	gnu.org
14	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils']	gnu.org
15	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils']	translationproject.org
16	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chmod.coreutils']	gnu.org
17	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils']	gnu.org
18	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils']	gnu.org
19	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils']	translationproject.org
20	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/chown.coreutils']	gnu.org
21	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils']	gnu.org
22	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils']	gnu.org
23	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils']	translationproject.org
24	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cp.coreutils']	gnu.org
25	http://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cpio.cpio']	gnu.org
26	http://www.gnu.org/software/cpio	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cpio.cpio']	gnu.org
27	http://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/cpio.cpio']	gnu.org
28	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils']	gnu.org
29	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils']	gnu.org
30	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils']	translationproject.org
31	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/date.coreutils']	gnu.org
32	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils']	gnu.org
33	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils']	gnu.org
34	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils']	translationproject.org
35	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/dd.coreutils']	gnu.org
36	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils']	gnu.org
37	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils']	gnu.org
38	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils']	translationproject.org
39	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/echo.coreutils']	gnu.org
40	https://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils']	gnu.org
41	https://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils']	gnu.org
42	https://translationproject.org/team	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils']	translationproject.org
43	https://www.gnu.org/software/coreutils	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/false.coreutils']	gnu.org
44	http://gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep']	gnu.org
45	http://www.gnu.org/software/grep	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep']	gnu.org
46	http://www.gnu.org/gethelp	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep']	gnu.org
47	http://git.sv.gnu.org/cgit/grep.git/tree/AUTHORS	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/grep.grep']	gnu.org
48	https://www.gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/gunzip.gzip']	gnu.org
49	https://www.gnu.org/licenses/gpl.html	['sample_C5.zip', 'BB6648.img', 'partition-0/initrd', 'bin/gzip.gzip']	gnu.org

C5 infoleak-urls

Figure 140: C5 Infoleak URLs (Black Duck)

Compone	Version	Latest ver	CVE	Matching type	CVSS	CVE publication date	Object compilation date	Object	Object full path	Object SHA1	CVSS3	CVSS vect
bash	4.4.23	5.2.15	CVE-2019-18276	Exact match		3.8 2019-11-29T14:52:13Z	2020-02-02T05:06:07Z	bash.bash	sample_C5.zip:BB6648.img:partition-0/initrd:bin/bash.bash	6e6b787521c26c016a8322a0008323436349864	7.8	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
bash	4.4.23	5.2.15	CVE-2022-3715	Exact match		3 2023-01-06T12:22:07Z	2020-02-02T05:06:07Z	bash.bash	sample_C5.zip:BB6648.img:partition-0/initrd:bin/bash.bash	6e6b787521c26c016a8322a0008323436349864	5.1	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:P/RL:W/RC:C
bind	9.11.4	9.18.17	CVE-2020-8625	Exact match		5 2021-02-19T16:26:05Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	7.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8625	Exact match		5 2021-02-19T16:26:05Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	7.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8625	Exact match		5 2021-02-19T16:26:05Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	7.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2018-5744	Exact match		4.7 2019-05-08T10:19:45Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	5.7	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2018-5744	Exact match		4.7 2019-05-08T10:19:45Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	5.7	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2018-5744	Exact match		4.7 2019-05-08T10:19:45Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.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/RC:
bind	9.11.4	9.18.17	CVE-2020-8617	Exact match		4.1 2020-05-21T13:21:07Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	7	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8617	Exact match		4.1 2020-05-21T13:21:07Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	7	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8617	Exact match		4.1 2020-05-21T13:21:07Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	7	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2021-25216	Exact match		3.8 2021-04-29T13:57:03Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	7.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2021-25216	Exact match		3.8 2021-04-29T13:57:03Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	7.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8616	Exact match		3.7 2020-05-20T15:52:58Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	7.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8616	Exact match		3.7 2020-05-20T15:52:58Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	7.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8616	Exact match		3.7 2020-05-20T15:52:58Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	7.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2023-2828	Exact match		3.7 2023-06-22T11:56:02Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2023-2828	Exact match		3.7 2023-06-22T11:56:02Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2023-2828	Exact match		3.7 2023-06-22T11:56:02Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-38178	Exact match		3.7 2022-09-22T15:46:27Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-38178	Exact match		3.7 2022-09-22T15:46:27Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-38178	Exact match		3.7 2022-09-22T15:46:27Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-38177	Exact match		3.7 2022-09-22T14:31:16Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-38177	Exact match		3.7 2022-09-22T14:31:16Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-38177	Exact match		3.7 2022-09-22T14:31:16Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-3094	Exact match		3.7 2023-01-26T16:51:17Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-3094	Exact match		3.7 2023-01-26T16:51:17Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-3094	Exact match		3.7 2023-01-26T16:51:17Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0667	Exact match		3.7 2022-03-17T14:41:48Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0667	Exact match		3.7 2022-03-17T14:41:48Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0667	Exact match		3.7 2022-03-17T14:41:48Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0635	Exact match		3.7 2022-03-17T16:51:31Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0635	Exact match		3.7 2022-03-17T16:51:31Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0635	Exact match		3.7 2022-03-17T16:51:31Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0396	Exact match		3.7 2022-03-17T14:46:59Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0396	Exact match		3.7 2022-03-17T14:46:59Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2022-0396	Exact match		3.7 2022-03-17T14:46:59Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2021-25215	Exact match		3.7 2021-04-29T13:48:40Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2021-25215	Exact match		3.7 2021-04-29T13:48:40Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2021-25215	Exact match		3.7 2021-04-29T13:48:40Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8623	Exact match		3.7 2020-08-21T11:03:23Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8623	Exact match		3.7 2020-08-21T11:03:23Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2020-8623	Exact match		3.7 2020-08-21T11:03:23Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2019-6465	Exact match		3.7 2019-05-14T11:02:26Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2019-6465	Exact match		3.7 2019-05-14T11:02:26Z	2020-02-02T05:14:43Z	libisc.so.169.0.3	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisc.so.169.0.3	a98564d06a9bd4071a82270acc2940095f75c63	6.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2019-6465	Exact match		3.7 2019-05-14T11:02:26Z	2020-02-02T05:14:43Z	libisccfg.so.160.2.1	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libisccfg.so.160.2.1	92431d1b6ffeb31a5df969ca3d31b65b44dfbf9b	6.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:
bind	9.11.4	9.18.17	CVE-2018-5743	Exact match		3.7 2019-04-29T13:57:32Z	2020-02-02T05:14:43Z	libbind9.so.160.0.8	sample_C5.zip:BB6648.img:partition-0/initrd:usr/lib64/libbind9.so.160.0.8	95a5b0b9fa2fa985912243404af647052edf210b5	6.5	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:

Figure 141: C5 CVEs (Black Duck)

Sample C5 Code Sentry Scan Report Excerpts

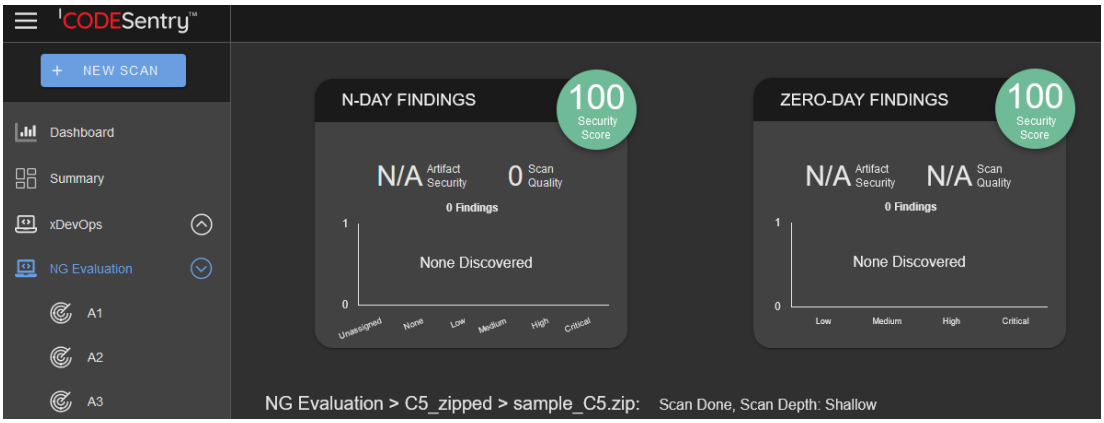


Figure 142: C5 Scan Overview (Code Sentry)

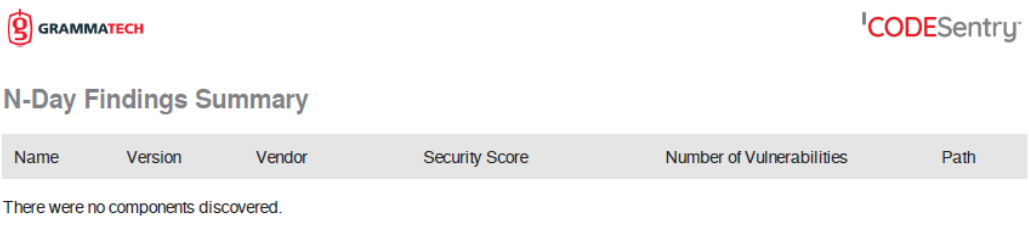


Figure 143: C5 N-day findings (Code Sentry)

GRAMMATECH CODESentry

N-Day Findings

Findings for sample_C5.zip

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

Figure 144: C5 Vulnerabilities (Code Sentry)

GRAMMATECH CODESentry

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")	-

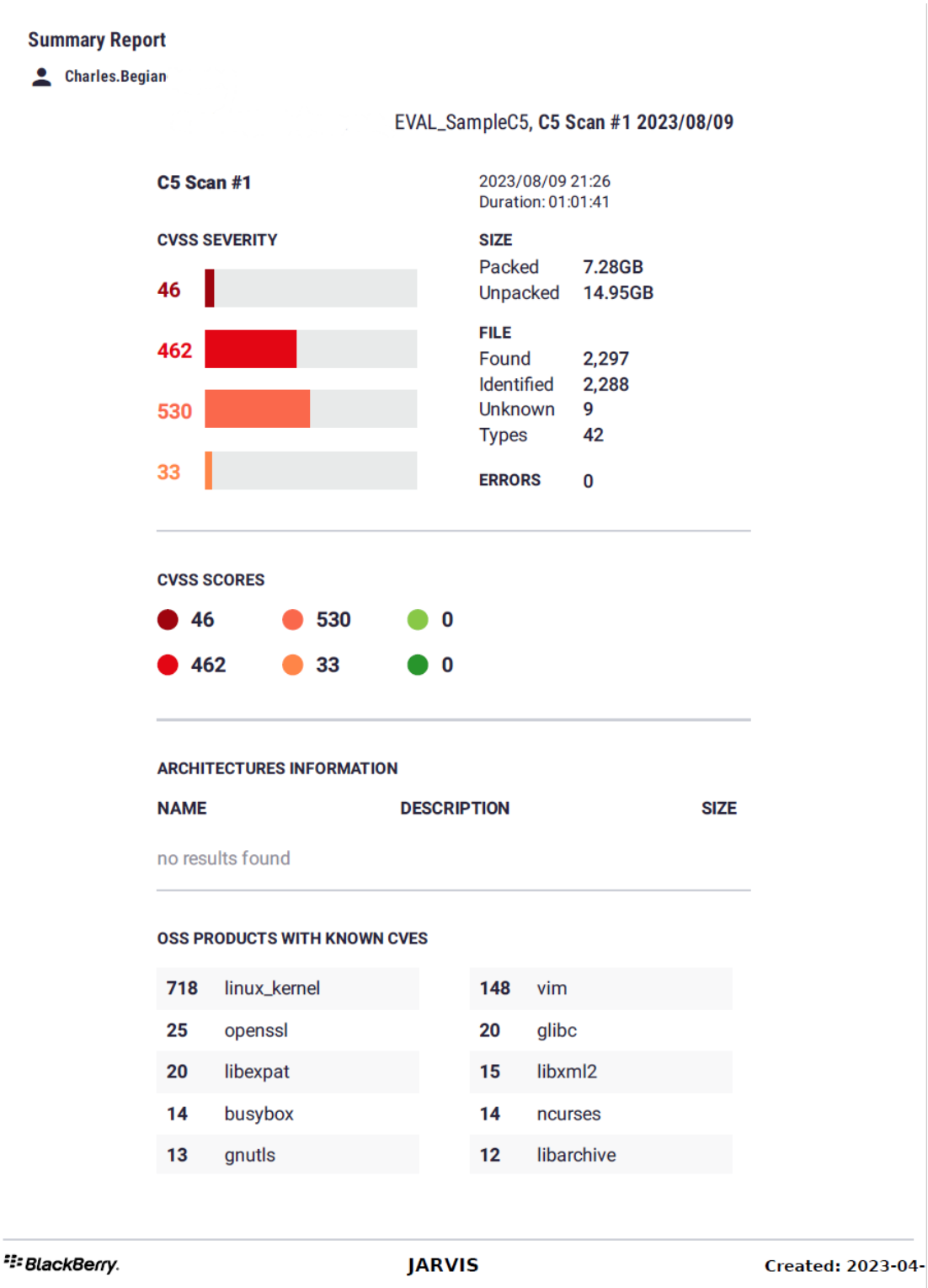
All Other CWE Findings (Excluding Top 25 CWEs)

Severity	Score	CWE ID	Name	Instances

None

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

Sample C5 Jarvis Scan Report Excerpts



Summary Report

Charles.Begian

EVAL_SampleC5, **C5 Scan #1 2023/08/09**

C5 Scan #1

2023/08/09 21:26
Duration: 01:01:41

CVSS SEVERITY

46
462
530
33

SIZE

Packed	7.28GB
Unpacked	14.95GB

FILE

Found	2,297
Identified	2,288
Unknown	9
Types	42

ERRORS 0

CVSS SCORES

46	530	0
462	33	0

ARCHITECTURES INFORMATION

NAME	DESCRIPTION	SIZE

no results found

OSS PRODUCTS WITH KNOWN CVES

718	linux_kernel	148	vim
25	openssl	20	glibc
20	libexpat	15	libxml2
14	busybox	14	ncurses
13	gnutls	12	libarchive

BlackBerry. JARVIS Created: 2023-04-

Figure 146: C5 Scan Overview (Jarvis)

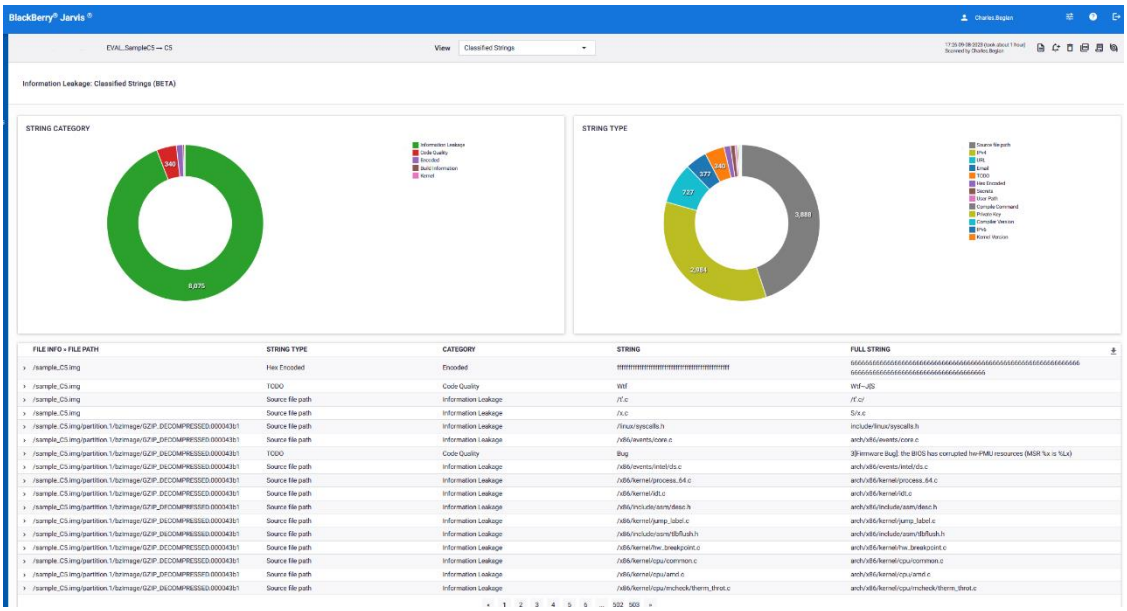


Figure 147: C5 Information leakage (Jarvis)

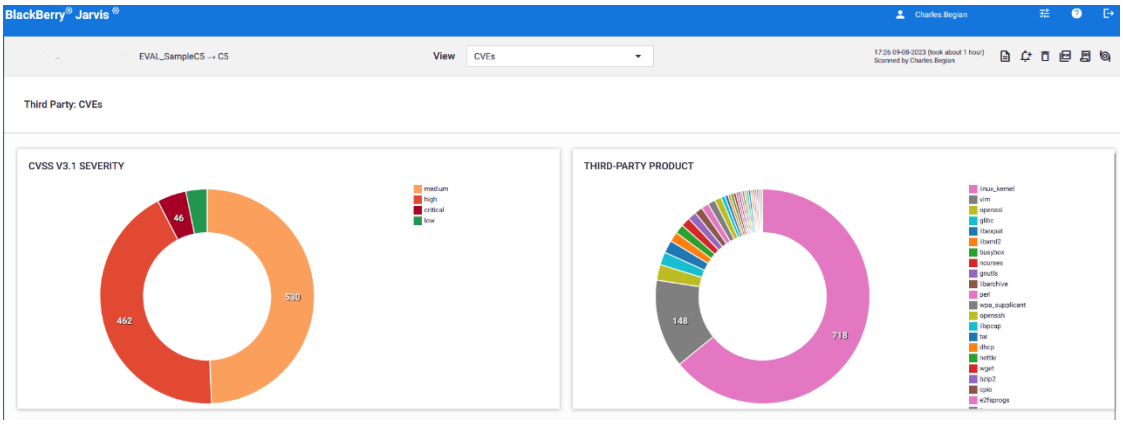


Figure 148: CVSS Severity Report (Jarvis)

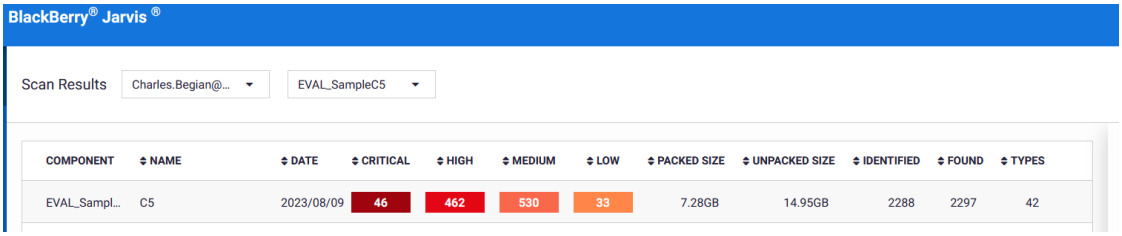


Figure 149: C5 CVE Summary by Severity (Jarvis)

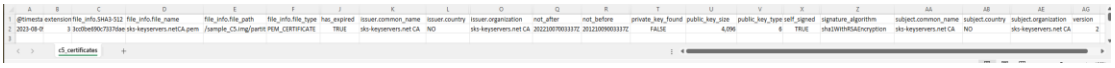


Figure 150: C5 Certificates Report (Jarvis)

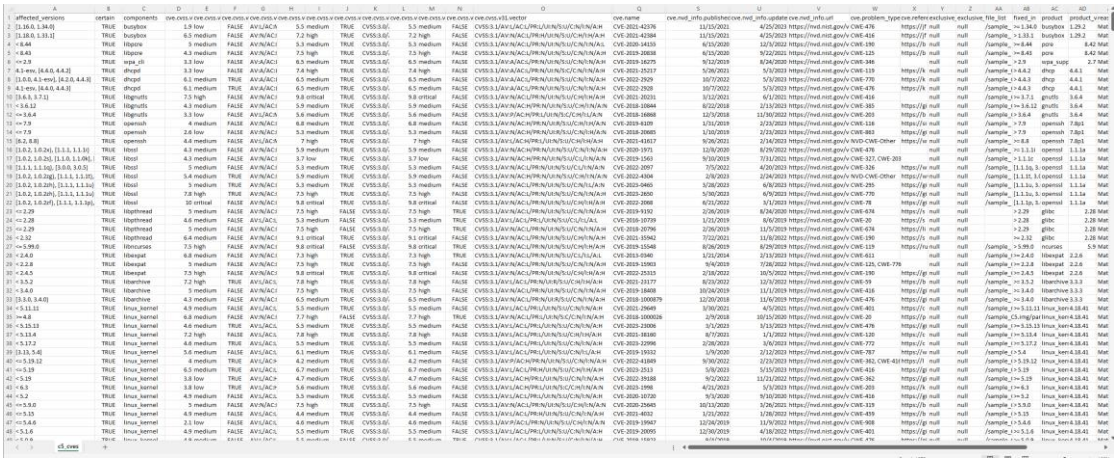


Figure 151: C5 CVEs (Jarvis)

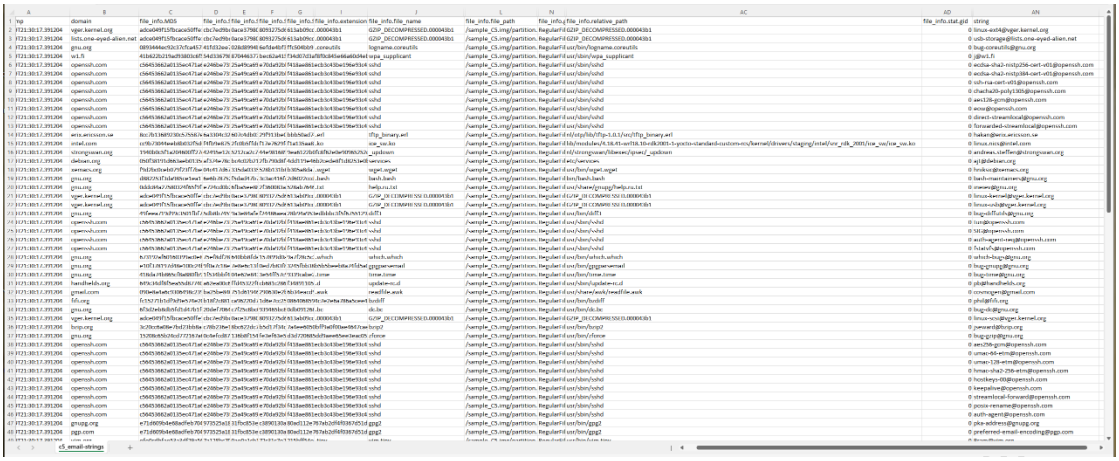


Figure 152: C5 email addresses (Jarvis)

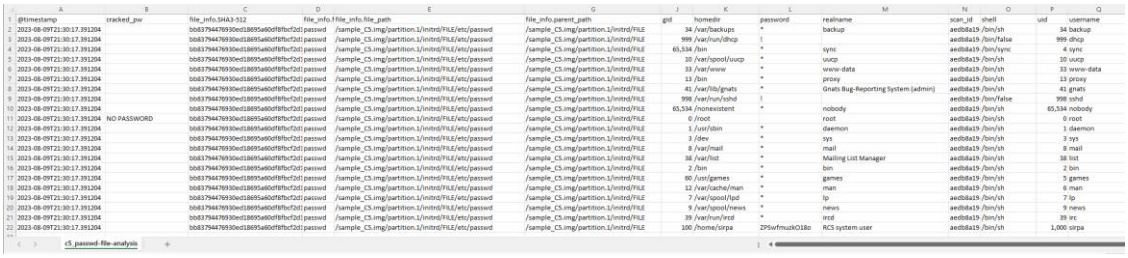


Figure 153: C5 Password File Analysis (Jarvis)

Figure 154: C5 Infoleak URL Report (Jarvis)

APPENDIX H: EFFECT OF ALGORITHM CHANGES

Artifact Risk Summary
Published: September 01, 2023

Evaluation Sample 6 / Test

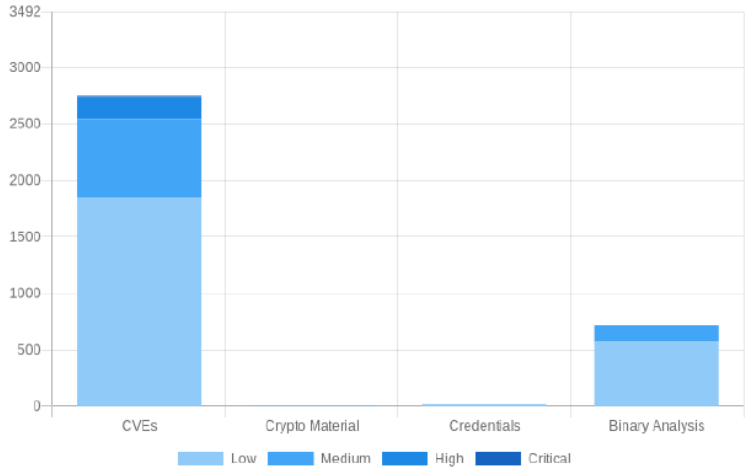
FINITE STATE

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 **Helpful Info** 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.

Artifact Risk Summary
Published: August 31, 2023

C2 / TEST

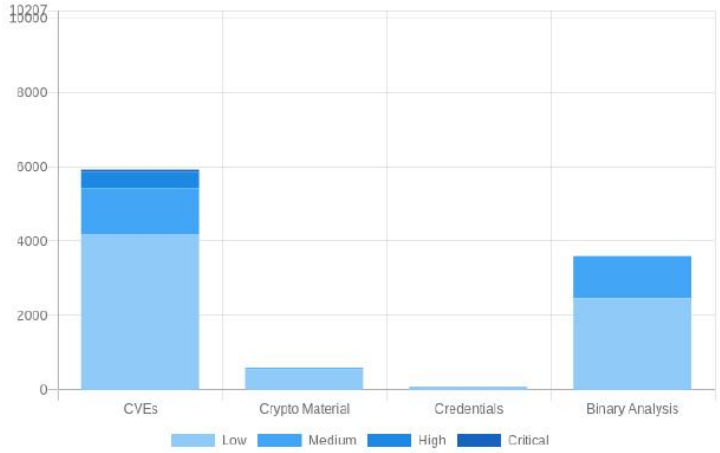
FINITE STATE

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.

10207 Findings by Type Breakdown



Looking for definitions? At the end of this report is a **Helpful Info** section.

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.