UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Melhoria ao Sistema de Avaliação de Vulnerabilidades - CVSS

Vanessa Rodrigues dos Santos

Mestrado em Segurança Informática

Dissertação orientada por:
Prof.ª Doutora Ana Luísa do Carmo Correia Respício
Prof.ª Doutora Maria Dulce Pedroso Domingos

2018

Agradecimentos

Quero agradecer às minhas orientadoras, Dulce Domingos e Ana Respício, pela orientação e conhecimento transmitido, que me ajudou na concretização deste trabalho.

Agradeço ao Grupo EDP, que me facultou a informação das vulnerabilidades de segurança nos seus sistemas e aplicações, tendo enriquecido exceptionalmente a minha dissertação.

Não poderia deixar de agradecer ao meu orientador de estágio na EDP, Pedro Rodrigues, pela disponibilidade, passagem de conhecimento, companheirismo e apoio demonstrado tanto ao longo do estágio como posteriormente. Foi uma excelente oportunidade no meu primeiro contato com a vida profissional e um bom começo para o desenvolvimento da minha tese. Também quero agradecer à Cátia Silva, Ivo Rosa e Gonçalo Martins, pelos momentos de companheirismo e apoio ao longo deste percurso.

Agradeço à minha grande amiga, Joana Ribeiro, por me mostrar que tudo é possível na vida. Seres tão positiva e estares sempre bem-disposta encorajou-me a continuar a tentar.

Um agradecimento especial aos meus queridos pais, Orlando Santos e Paula Santos, que sempre me apoiaram e me deram força e energia para continuar a lutar pelos meus objetivos de vida. Sem vocês, este objetivo seria impossível de se concretizar.

À minha irmã, Nicole Santos, que agradeço do fundo do meu coração! Sei que estive muito ausente e se não fosses tão compreensiva e flexível, nada disto seria possível. Obrigada por teres sido tão adulta nos momentos em que precisei que assim o fosses.

Agradeço ao resto da minha família, em especial à minha avó Hortense, que é e sempre será a minha estrelinha da sorte.

Last but not least, ao meu marido, Pedro Maia, que esteve sempre ao meu lado e caminhou comigo até ao fim desta jornada. Sem ti, não seria a mesma coisa.

Aos meus Pais e Irmã.

Resumo

O número de vulnerabilidades identificadas e reportadas tem vindo a aumentar ao longo dos últimos anos e deste modo a priorização de vulnerabilidades torna-se bastante complexa de gerir. Vários sistemas de avaliação foram propostos para colmatar esta adversidade, sendo o mais conhecido e adotado, o *Common Vulnerability Scoring System (CVSS)*.

Foram identificados alguns problemas no CVSS, sendo estes, a reduzida diversidade de valores obtidos na avaliação e a existência de uma grande quantidade de vulnerabilidades nas classificações crítica e alta.

Neste sentido, é proposto uma extensão ao CVSS que pretende aumentar a diversidade de valores e diminuir a quantidade de vulnerabilidades nas classificações crítica e alta. Desta forma, são propostos dois novos valores para os fatores de impacto na confidencialidade, integridade e disponibilidade do CVSS referentes à métrica base.

A proposta foi avaliada recorrendo a dados disponibilizados pelo *National Vulnerability Database (NVD)* e pela Energias de Portugal (EDP). Deste modo, as amostragens retiradas das duas fontes foram reavaliadas considerando os valores propostos e comparadas com os valores por omissão do CVSS.

Palavras-chave:Vulnerabilidades, Avaliação de vulnerabilidades, CVSS, Normas, Ataques Cibernéticos, Risco, Priorização

Abstract

The number of identified and reported vulnerabilities has been increasing over the past few years and thus prioritizing vulnerabilities becomes quite complex to manage. Several evaluation systems have been proposed to address this adversity, being the Common Vulnerability Scoring System (CVSS) best known and adopted.

Some issues were identified in the evaluation of vulnerabilities using CVSS. The diversity of values obtained is one of them, since the number of vulnerabilities in certain classifications is exceptionally higher than others. Another issue is the large number of vulnerabilities in the critical and high classifications.

In this sense, it is proposed an extension to the CVSS that intends to increase the diversity of values and to reduce the amount of vulnerabilities in the critical and high classifications. Therefore, two new values are proposed for the CVSS confidentiality, integrity and availability factors for the base metric.

The proposal was evaluated using data provided by the National Vulnerability Database (NVD) and by Energias de Portugal (EDP). Thus, the samplings taken from the two sources were re-evaluated considering the proposed values and compared with the CVSS default values.

Keywords:Vulnerabilities, Vulnerability scoring, CVSS, Standards, Cyber Attacks, Risk, Prioritization

Conteúdo

Lista de Figuras **xii**

Lista de Tabelas **xv**

1 Introdução **1**
1.1 Motivação 1
1.2 Objetivos 3
1.3 Contribuições 4
1.4 Estrutura do documento 4

2 Trabalho relacionado **5**
2.1 CVSS – Common Vulnerability Scoring System 5
2.2 WIVSS – Weighted Impact Vulnerability Scoring System 14
2.3 VRSS – Vulnerability Rating and Scoring System 18
2.4 OWASP – Risk Rating Methodology 22
2.5 CWSS – Common Weakness Scoring System 30
2.6 Análise das metodologias apresentadas 32

3 Apresentação de uma proposta de melhoria ao CVSS **35**
3.1 Análise do sistema de avaliação de vulnerabilidades - CVSS 35
3.1.1 Quantidade de vulnerabilidades nas classificações críticas e altas . 35
3.1.2 Diversidade de valores 36
3.2 Definição de critérios 40
3.3 Proposta de um novo valor 40
3.3.1 Métrica Base - Análise das métricas em concordância com os critérios definidos 41
3.3.2 Métrica Ambiental - Análise das métricas em concordância com os critérios definidos 43
3.4 Proposta de um segundo valor 45
3.4.1 Métrica Base - Análise das métricas em concordância com os critérios definidos 45

3.4.2 Métrica Ambiental - Análise das métricas em concordância com os critérios definidos 46
3.5 Definição dos novos valores 49
3.6 Resumo 52

4 Avaliação e resultados **55**
4.1 Vulnerabilidades NVD 55
4.1.1 Classificação crítica 56
4.1.2 Classificação alta 57
4.2 Vulnerabilidade EDP 58
4.2.1 Classificação crítica 59
4.2.2 Classificação alta 60
4.2.3 Comparação dos resultados com a severidade das vulnerabilidades 61
4.3 Resumo 63

5 Conclusão e Trabalho futuro **65**
5.1 Conclusão 65
5.2 Trabalho futuro 65

Bibliografia **71**

A Avaliação das vulnerabilidades **73**
A.1 NVD 73
A.1.1 Classificação crítica 73
A.1.2 Classificação alta 77
A.2 Grupo EDP 82
A.2.1 Classificação crítica 82
A.2.2 Classificação alta 102

Lista de Figuras

2.1 Equações da ”métrica base”(*base metric*) do CVSS v3, extraído de [9] . . 9
2.2 Equações da ”métrica temporal” (*temporal metric*) do CVSS v3, extraído de [9] 11
2.3 Equações da ”métrica ambiental” (*environmental metric*) do CVSS v3, extraído de [9] 12
2.4 Algoritmo WIVSSv2, extraído de [45] 17
2.5 Estatísticas e distribuição de valores WIVSSv2, extraído de [45] 18
2.6 VRSS - Qualitativa e Quantitativa, extraído de [13] 19
2.7 VRSS - Mapeamento do modelo qualitativo para o quantitativo, extraído de [13] 19
2.8 VRSS - Sistema de avaliação de vulnerabilidades, extraído de [14] 20
2.9 VRSS - Framework v2, extraído de [14] 21
2.10 Top 10 das vulnerabilidades mais severas, extraído de [32] 23
2.11 Níveis de Verosimilhança e Impacto [31] 30
2.12 Severidade do risco [31] 30

3.1 Número de vulnerabilidades por níveis de classificação - comparação entre versão 2 e versão 3 do CVSS 36
3.2 Distribuição de valores - Métrica base com os 3 valores por defeito 38
3.3 Distribuição de valores - Métrica base e ambiental com os 3 valores por defeito 40
3.4 Distribuição de valores em proporção - Métrica base com os 3 valores por defeito e a adição do valor 0.32 43
3.5 Distribuição de valores em proporção - Métrica Ambiental com os 3 valores por defeito e o novo valor 0.32 45
3.6 Contabilização de *Scores* da métrica base com cinco valores na sub-métrica impacto 46
3.7 Contabilização de *Scores* da métrica ambiental com cinco valores na sub-métrica impacto 47
3.8 Distribuição de valores em proporção - Métrica Base com os 3 valores por defeito e os novos valores 48

3.9 Distribuição de valores em proporção - Métrica Ambiental com os 3 valores por defeito e os novos valores 48
3.10 Distribuição de valores na classificação alta em proporção - Métrica Base com os novos valores e os por omissão 48
3.11 Distribuição de valores na classificação alta em proporção - Métrica Ambiental com os novos valores e os por omissão 48
3.12 Distribuição de valores na classificação crítica em proporção - Métrica Base com os novos valores e os por defeito 49
3.13 Distribuição de valores na classificação crítica em proporção - Métrica Ambiental com os novos valores e os por defeito 49

4.1 Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - NVD 57
4.2 Diminuição da classificação crítica para valores da classificação alta - NVD 57
4.3 Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - NVD 58
4.4 Diminuição da classificação alta para valores da classificação média - NVD 58
4.5 Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - EDP 60
4.6 Diminuição da classificação crítica para valores da classificação alta - EDP 60
4.7 Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - EDP 60
4.8 Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - EDP 61
4.9 Percentagem de vulnerabilidade por cada nível de severidade - Empresa externa 62
4.10 Percentagem de vulnerabilidade por cada nível de severidade - CVSS . . 62
4.11 Percentagem de colisões por classificação - após reavaliação 63

Lista de Tabelas

2.1 ”Métrica Base” (*Base Metric*) - ”Superfície de ataque” (*Attack Vector*) [8] 7
2.2 ”Métrica Base” (*Base Metric*) - ”Complexidade do ataque” (*Attack Complexity*) [8] 7
2.3 ”Métrica Base” (*Base Metric*) - ”Privilégios requeridos” (*Privilege Required*) [8] 7
2.4 ”Métrica Base” (*Base Metric*) - ”Interação do utilizador” (*User Interaction*) [8] 8
2.5 ”Métrica Base” (*Base Metric*) - ”Impacto na Confidencialidade” (*Confidentiality Impact*) [8] 8
2.6 ”Métrica Base” (*Base Metric*) - ”Impacto na Integridade” (*Integrity Impact*) [8] 8
2.7 ”Métrica Base” (*Base Metric*) - ”Impacto na Disponibilidade” (*Availability Impact*) [8] 9
2.8 ”Métrica Temporal” (*Temporal Metric*) – Maturidade do código de exploração (*Exploit Code Maturity*) [8] 10
2.9 ”Métrica Temporal” (*Temporal Metric*) - Nível de remediação (*Remediation level*) [8] 10
2.10 ”Métrica Temporal” (*Temporal Metric*) - Grau de confiança (*Report Confidence*) [8] 10
2.11 ”Métrica Ambiental” (*Environmental Metric*) - ”Requisitos na confidencialidade” (*Confidentiality Requirement*) [8] 11
2.12 ”Métrica Ambiental” (*Environmental Metric*) - ”Requisitos na integridade” (*Integrity Requirement*) [8] 11
2.13 ”Métrica Ambiental” (*Environmental Metric*) - ”Requisitos na disponibilidade” (*Availability Requirement*) [8] 12
2.14 Mapeamento dos valores quantitativos em qualitativos [8] 13
2.15 Representação textual de cada grupo de métricas, extraído de [8] 13
2.16 Os *scores* definidos na métrica base (*base metric*) no CVSS v2 [46] . . . 14
2.17 Os *scores* definidos na métrica base (*base metric*) no WIVSS [46] 15
2.18 Os valores escolhidos para a sub-métrica de impacto da métrica base (*base metric*) do WIVSSv2 [45] 18

2.19 AHP - Valores encontrados para cada tipo de vulnerabilidade (VTF) considerado 22
2.20 OWASP: Fatores inerentes à ameaça - Nível de Perícia [31] 25
2.21 OWASP: Fatores inerentes à ameaça - Motivação [31] 25
2.22 OWASP: Fatores inerentes à ameaça - Oportunidade [31] 25
2.23 OWASP: Fatores inerentes à ameaça - Dimensão [31] 25
2.24 OWASP: Fatores inerentes à vulnerabilidade - Facilidade na identificação [31] 26
2.25 OWASP: Fatores inerentes à vulnerabilidade - Facilidade na exploração [31] 26
2.26 OWASP: Fatores inerentes à vulnerabilidade - Conhecimento [31] 26
2.27 OWASP: Fatores inerentes à vulnerabilidade - Deteção da Intrusão [31] . 26
2.28 OWASP: Fatores inerentes ao impacto técnico - Perda na Confidencialidade [31] 27
2.29 OWASP: Fatores inerentes ao impacto técnico - Perda na Integridade [31] 28
2.30 OWASP: Fatores inerentes ao impacto técnico - Perda na Disponibilidade [31] 28
2.31 OWASP: Fatores inerentes ao impacto técnico - Perda na responsabilidade [31] 28
2.32 OWASP: Fatores inerentes ao impacto técnico - Prejuízo Financeiro [31] . 28
2.33 OWASP: Fatores inerentes ao impacto técnico - Prejuízo na Reputação [31] 29
2.34 OWASP: Fatores inerentes ao impacto técnico - Não Cumprimento [31] . 29
2.35 OWASP: Fatores inerentes ao impacto técnico - Violação na Privacidade [31] 29

3.1 Contabilização de *Scores* da métrica base e ambiental com quatro valores na sub-métrica impacto 42
3.2 Métricas para a escolha do quarto valor comparativamente ao valores por defeito - Métrica Base - percentagem de valores nas classificações qualitativas e curtose 43
3.3 Métricas para a escolha do quarto valor comparativamente aos valores por defeito - Métrica Ambiental - percentagem de valores nas classificações qualitativas e Curtose 44
3.4 Métrica Base - Impacto na Confidencialidade, Integridade e disponibilidade 44
3.5 Métricas para a escolha do quinto valor - Métrica Base - percentagem de valores nas classificações qualitativas e Curtose 46
3.6 Métricas para a escolha do quinto valor - Métrica Ambiental - percentagem de valores nas classificações e Curtose 47
3.7 Métrica Base - Impacto na confidencialidade, integridade e disponibilidade 49

4.1 Mapeamento entre a criticidade do ativo e os requisitos na confidencialidade, integridade e disponibilidade 59

A.1 Avaliação das vulnerabilidades classificação crítica - NVD 77
A.2 Avaliação das vulnerabilidades classificação alta - NVD 81
A.3 Sumário das vulnerabilidades na classificação crítica - Grupo EDP 86
A.4 Avaliação das vulnerabilidades na classificação crítica - Grupo EDP . . . 96
A.5 Classificações das vulnerabilidades na classificação crítica - Grupo EDP . 101
A.6 Sumário das vulnerabilidades classificação alta - Grupo EDP 106
A.7 Avaliação das vulnerabilidades na classificação alta - Grupo EDP 116
A.8 Classificações das vulnerabilidades na classificação alta - Grupo EDP . . 121

Capítulo 1

Introdução

"When every defect is high priority... Nothing is!"

[39]

1.1 Motivação

Em Segurança Informática, uma vulnerabilidade é uma fraqueza existente num sistema, aplicação, serviço, dispositivo que pode ser explorada por uma ou mais ameaças e como resultado causar impacto na confidencialidade, integridade ou disponibilidade dos dados ou sistema em causa [42, 18].

O número de vulnerabilidades identificadas está a aumentar exponencialmente nos últimos anos. Em 1999, foram identificadas 894 vulnerabilidades em que 164 foram consideradas críticas [3], no entanto em Setembro de 2017, foram contabilizadas 10679 vulnerabilidades em que 1119 são consideradas críticas [4]. Estas vulnerabilidades devem ser tratadas o quanto antes pois causam um impacto total na confidencialidade, integridade e disponibilidade no componente vulnerável dentro da organização.

Vários ataques cibernéticos foram surgindo nos últimos anos, como por exemplo o *Stuxnet*, um *worm* desenhado para infetar produtos da Siemens PCS 7 [1] - SIMATIC WinCC [2] e PLCs [3] [1]. Este *worm* foi inserido em várias infraestruturas, entre as quais destaca-se a central nuclear no Irão, em que foram destruídas as centrifugadoras que enriqueciam urânio. Este *worm* foi desenvolvido com o propósito de alterar bits nos PLCs de modo a aumentar a velocidade máxima definida para as centrifugadoras rodarem. Outro ataque cibernético bem mais recente, em Maio de 2017, e que também teve bastante visibilidade foi o *WannaCry* [40, 43], um tipo de *malware* designado por *Ransomware*, que explora uma vulnerabilidade conhecida no protocolo *Server Message Block* (SMB)

[1] Sistema de controlo industrial

[2] Produto da Siemens para visualização, monitorização e controlo do processo de fabrico

[3] Controladores lógicos programáveis são sistemas de automação lógicos e físicos

versão 1 do Windows, com o propósito de se propagar na rede e deste modo infetar um grande número de computadores. Este *Ransomware* cifra os dados do computador e é exigida a transferência de uma quantia em *Bitcoins* para obter a chave de decifração e assim recuperar os dados. O ataque podia ter sido prevenido se fosse aplicado o *patch* de segurança disponibilizado pelo fabricante, a Microsoft, em Março de 2017. A vulnerabilidade no SMB, CVE-2017-0144, foi publicada em Março com um CVSS *score* de 9.3 em 10 [5], o que significa que esta vulnerabilidade estava classificada como crítica mas não lhe foi dada a devida importância.

Um papel importante, indispensável em qualquer organização, incide na gestão de vulnerabilidades de segurança. Esta função pode ajudar a diminuir a janela de oportunidade do atacante, contudo depende da abordagem utilizada para o efeito. Ao longo dos últimos anos, foram desenvolvidas várias metodologias para a avaliação de vulnerabilidades e a sua adoção nas organizações é essencial para precaver ciber ataques.

No passado, cada fabricante utilizava o seu próprio sistema de avaliação de vulnerabilidades para classificar as vulnerabilidades nos seus softwares, sem detalhar os critérios de avaliação [19]. Recentemente, vários fornecedores de serviços em segurança informática e organizações sem fins lucrativos desenvolveram, promoveram e implementaram sistemas de avaliação de vulnerabilidades. Contudo, não há coesão ou interoperabilidade entre esses sistemas e o âmbito é limitado [42].

O *Common Vulnerability Scoring System (CVSS)* foi inicialmente um projeto criado pelo *National Infrastructure Advisory Council (NIAC)* [22] e posteriormente delegado ao *Forum for Incident Response and Security Teams (FIRST)* [7] com o propósito de disponibilizar um sistema de avaliação de vulnerabilidades comum para toda a indústria, com o objetivo de auxiliar a determinar as vulnerabilidades mais severas, que devem ser mitigadas de imediato [22]. O *FIRST* conta com a participação dos elementos do *Common Vulnerability Scoring System-Special Interest Group (CVSS-SIG)* para melhoria contínua desta norma, sendo estes elementos inseridos em várias organizações, comunidades, centros de investigação, instituições de normas, com conhecimento de Segurança Informática, tais como, a Microsoft, Dell, CERT/CC [2], Intel, NIST [23]. Neste momento o CVSS está na versão 3 e é o sistema de avaliação de vulnerabilidades mais adotado pela indústria, por entidades reputadas como a Amazon, Arcsight, Cisco, IBM, McAfee, NIST, OpenVAS, RAPID7, Symantec, Qualys, entre outras.

Apesar da usabilidade desta norma e das melhorias significativas verificadas ao longo dos últimos 12 anos, com o suporte de um comité com bastante sabedoria e conhecimento em Segurança Informática, foram apresentados vários problemas na versão 3 do CVSS [35, 36, 37, 38, 39]. Um dos grandes problemas causa bastante impacto num dos objetivos principais da criação desta metodologia, pois se na versão 2 já existiam, em 2016, 2066 vulnerabilidades com classificações no nível alto, na versão 3 observou-se um aumento significativo na severidade das vulnerabilidades nos níveis alto e crítico, com 2066

e 894 respetivamente, totalizando 3082 vulnerabilidades e que corresponde ao nível alto na versão 2 do CVSS [39]. É de referir que na altura nem todas as vulnerabilidades tinham sido classificadas na versão 3 do CVSS e por este motivo a amostragem indicada anteriormente considera 5135 vulnerabilidades pontuadas na versão 2 e 4929 vulnerabilidades pontuadas na versão 3, o que significa que existem menos 209 vulnerabilidades na versão 3 e que por isso não foram consideradas na análise efetuada pelo *Risk Based Security (RBS)*. Como um dos objetivos desta norma é apoiar a indústria na priorização do tratamento de vulnerabilidades, este problema torna a gestão de vulnerabilidades uma tarefa difícil de alcançar dado que não se consegue justificar o tratamento das vulnerabilidades mais críticas visto que a maioria é classificada como tal - "When every defect is high priority... Nothing is!"[39]. Desta forma, as vulnerabilidades permanecem nas organizações por um grande período de tempo e suscetíveis de serem exploradas por um atacante. Na minha experiência profissional em avaliação da severidade das vulnerabilidades, verifiquei na prática o problema indicado anteriormente e por esse motivo senti dificuldade em acelerar o processo de mitigação das vulnerabilidades e cumprir com os KPIs (*Key Performance Indicators*).

Para além do problema exposto anteriormente, existe pouca diversidade de valores em toda a escala dado que existem várias classificações que não são obtidas na avaliação da severidade das vulnerabilidades e outras classificações que são obtidas em demasia, existindo uma heterogeneidade de valores notória. Este facto, também influencia na eficácia de tratamento das vulnerabilidades visto que quanto mais vulnerabilidades são classificadas com a mesma severidade, mais difícil é a priorização do seu tratamento.

Como já procedido nas versões anteriores do CVSS, que deram origem ao CVSS versão 3, foram propostas evoluções a esta versão e foi publicada, em Janeiro de 2018, uma lista de possíveis melhorias. Algumas destas melhorias já foram aprovadas para serem refletidas na versão 4 do mesmo [12]. No entanto, nenhuma das propostas endereça os problemas relativos à pouca diversidade de valores obtidos na avaliação e à grande quantidade de vulnerabilidades nas classificações crítica e alta. Por este motivo, surge a necessidade de propor uma melhoria a esta metodologia, considerando estes dois problemas, um dos quais, já bastante criticado [33].

1.2 Objetivos

O presente trabalho de dissertação tem como principal objetivo melhorar o CVSS versão 3, aumentando a diversidade de valores e diminuindo a quantidade de vulnerabilidades que estão classificadas nos valores críticos e altos.

Ao longo do trabalho e de acordo com o objetivo apresentado, pretende-se avaliar uma extensão ao CVSS, que passará pelos seguintes pontos:

1. Estudo do CVSS;

2. Estudo das metodologias para avaliação de vulnerabilidades baseadas no CVSS;

3. Análise das diferentes abordagens utilizadas em cada metodologia.

1.3 Contribuições

A contribuição deste trabalho é uma extensão ao CVSS que pretende melhorar a diversificação dos valores obtidos na avaliação de vulnerabilidades e diminuir o número de vulnerabilidades nos valores críticos e altos. Deste modo, vão ser propostos dois novos valores relativos aos fatores de impacto na confidencialidade, integridade e disponibilidade.

A validação da proposta apresentada foi efetuada utilizando uma amostra de vulnerabilidades do NVD [24] e uma amostra de vulnerabilidades disponibilizadas pelo parceiro EDP. Estas vulnerabilidades serão reavaliadas e comparadas com as classificações obtidas com os valores por omissão do CVSS.

Com esta melhoria, é pretendido facilitar a priorização de vulnerabilidades e respetiva mitigação por ordem de severidade. Como tal, possibilita a célere proteção de ataques intrusivos, como os mencionados no presente capítulo.

1.4 Estrutura do documento

Este documento está organizado da seguinte forma:

- Capítulo 2 – Trabalho relacionado: Neste capítulo vão ser apresentadas e descritas metodologias propostas com base no CVSS e também todos os detalhes desta norma.

- Capítulo 3 – Apresentação da proposta de melhoria ao CVSS: Vai ser abordado o problema em mais detalhe e proposta uma extensão de melhoria ao CVSS.

- Capítulo 4 - Avaliação e resultados: Validação da extensão proposta e apresentação dos resultados obtidos comparativamente às classificações do CVSS.

- Capítulo 5 - Conclusão e Trabalho futuro: Vão ser expostas as conclusões ao trabalho realizado e identificado o trabalho futuro para a melhoria contínua do CVSS.

Capítulo 2

Trabalho relacionado

Um sistema de avaliação de vulnerabilidades torna-se essencial para as organizações devido ao elevado número de vulnerabilidades que são identificadas dia após dia. É necessário diferenciar as vulnerabilidades mais críticas das menos críticas para o negócio da organização e por este motivo, foram criados vários sistemas para avaliação de vulnerabilidades, com o objetivo de auxiliar as organizações nesta complexa função.

Os três tipos de metodologias existentes são qualitativa, quantitativa e híbrida [45]. A metodologia qualitativa é utilizada para classificar cada vulnerabilidade com diferentes níveis de severidade, como por exemplo, baixo, médio, alto. A metodologia quantitativa é utilizada para pontuar cada vulnerabilidade com um valor calculado por uma ou mais fórmulas construídas para o efeito. Uma metodologia híbrida é a junção das duas metodologias mencionadas anteriormente, em que é classificada qualitativamente a severidade da vulnerabilidade e consoante o nível de classificação é pontuada, ou vice versa.

A metodologia mais conhecida e utilizada é o Common Vulnerabilities Scoring System (CVSS) mantida pelo Forum for Incident Response and Security Teams (FIRST) e encontra-se na versão 3. É uma metodologia híbrida, dividida em três métricas: a "Base" (*Base*) direcionada a fatores inerentes à exploração da vulnerabilidade, a "Temporal" (*Temporal*) direcionada a fatores inerentes à vulnerabilidade que sofrem modificações ao longo do tempo, e por último, a "Ambiental" (*Environmental*) focada em fatores relacionados com o ativo e o ambiente onde está inserido na organização. Para além do CVSS, foram desenvolvidas várias metodologias, algumas para melhorar o CVSS versão 2.

Neste capítulo vão ser apresentadas algumas destas metodologias, descrevendo e analisando cada proposta que se baseia no CVSS.

2.1 CVSS – Common Vulnerability Scoring System

O Common Vulnerability Scoring System (CVSS) é uma metodologia utilizada para avaliação de vulnerabilidades com o objetivo de auxiliar as organizações a priorizar as

vulnerabilidades relativamente à severidade. Esta metodologia foi criada pelo NIAC e posteriormente delegado ao FIRST. Este é constituído por várias equipas de resposta a incidentes de segurança provenientes de várias organizações.

A metodologia CVSS já foi revista duas vezes, encontrando-se neste momento na versão 3. Antes da publicação da versão 3 da norma foi previamente analisada por vários elementos de diversas organizações. No entanto, a versão 1 não foi revista por um grande *quorum* e por este motivo, identificaram vários problemas o que resultou em inúmeras propostas de melhoria aos pontos fracos identificados nesta versão [16]. As propostas aceites foram aplicadas ao CVSS versão 1 e desta forma foi publicada a versão 2 em 2007 [16].

A participação dos elementos do CVSS-SIG (Common Vulnerability Scoring System-Special Interest Group) foi um contributo essencial na revisão e melhoria do CVSS, no qual investiram várias horas efetuando testes a centenas de vulnerabilidades. Este esforço dos elementos do CVSS-SIG resultou numa melhoria significativa na fiabilidade, flexibilidade e usabilidade da metodologia [44].

A versão 2 foi uma grande ajuda na avaliação e priorização de vulnerabilidades, tendo sido adotada por várias entidades reputadas, como a Amazon, Arcsight, Cisco, IBM, McAfee, NIST, OpenVAS, RAPID7, Symantec, Qualys, entre outras. Apesar das melhorias significativas na versão 2, comparativamente à versão 1, foram apresentadas dificuldades em pontuar vulnerabilidades que a sua exploração impactasse outro componente para além do componente vulnerável [10]. Por este motivo, na versão 3, foi adicionado um novo fator à métrica base, denominado por ”âmbito” (*scope*).

Foi inserido um novo valor ao fator ”superfície de ataque” (*Attack Vector*), denominado por ”físico” (*physical*). Com este valor é possível diferenciar vulnerabilidades que requerem acesso local de vulnerabilidades que requerem acesso físico. Outro fator também inserido na métrica base, é denominado por ”interação do utilizador” (*user interaction*), que consoante seja necessário algum tipo de interação de utilizadores para uma exploração bem sucedida, diminui o peso atribuído a este fator, o que nas versões anteriores não era considerado. A ”autenticação” (*Authentication*) foi substituída por ”privilégios requeridos” (*Privilege Required*). Em vez de existir uma contagem relativa ao número de autenticações necessárias para explorar uma vulnerabilidade, é necessário avaliar o nível de privilégios requeridos. Os impactos na confidencialidade, integridade e disponibilidade são agora pontuados pelo nível de impacto em vez da percentagem de impacto, ou seja, os valores ”parcial” (*partial*) e ”total” (*complete*) foram substituídos pelos valores ”baixo” (*low*) e ”alto” (*high*) respetivamente. Os fatores ”dano colateral potencial” (*collateral damage potential*) e ”distribuição alvo” (*target distribution*), da ”métrica ambiental” (*Environmental Metric*), foram substituídos pelos fatores modificados da ”métrica base” (*base metric*), ou seja, os valores da sub-métrica ”exploração” (*exploitability*) da ”métrica base” (*base metric*) podem ser alterados considerando o meio envolvente onde

o ativo está inserido no sistema.

Como já referido anteriormente, o CVSS versão 3 consiste em três grupos de métricas e a única obrigatória para o cálculo da severidade é a métrica base (*base metric*).

O ”Grupo da Métrica Base” (*Base Metric Group*) é constituído por duas sub-métricas, a sub-métrica ”exploração” (*exploitability*) e a sub-métrica ”impacto” (*impact*). A sub-métrica ”exploração” (*exploitability*) é composta pelos quatro fatores seguintes, que representam as caraterísticas do componente vulnerável:

1. ”Superfície de ataque” (*Attack Vector*): A partir de onde é que ocorre a exploração da vulnerabilidade. (Tabela 2.1)

2. ”Complexidade do ataque” (*Attack Complexity*): O esforço e tempo consumido. (Tabela 2.2)

3. ”Privilégios requeridos” (*Privilege Required*): O nível de privilégios necessário. (Tabela 2.3)

4. ”Interação do utilizador” (*User Interaction*): Requer interação de um ou mais utilizadores para além do atacante. (Tabela 2.4)

Opção	Valor	String
Rede (*Network*)	0.85	N
Rede Adjacente (*Adjacent Network*)	0.62	A
Local (*Local*)	0.55	L
Físico (*Physical*)	0.2	P

Tabela 2.1: ”Métrica Base” (*Base Metric*) - ”Superfície de ataque” (*Attack Vector*) [8]

Opção	Valor	String
Baixo (*Low*)	0.77	L
Alto (*High*)	0.44	H

Tabela 2.2: ”Métrica Base” (*Base Metric*) - ”Complexidade do ataque” (*Attack Complexity*) [8]

Opção	Valor	String
Nenhum (*None*)	0.85	N
Baixo (*Low*)	0.62 (0.68 se o âmbito (*scope*) altera)	L
Alto (*High*)	0.27 (0.50 se o âmbito (*scope*) altera)	H

Tabela 2.3: ”Métrica Base” (*Base Metric*) - ”Privilégios requeridos” (*Privilege Required*) [8]

Opção	Valor	String
Não requerido (*None*)	0.85	N
Requerido (*Required*)	0.62	R

Tabela 2.4: ”Métrica Base” (*Base Metric*) - ”Interação do utilizador” (*User Interaction*) [8]

A sub-métrica de ”impacto” (*impact*) é composta pelos três fatores seguintes, que representam a consequência da exploração bem-sucedida:

1. ”Impacto na confidencialidade” (*Confidentiality Impact*): Na medida em que o atacante ao explorar uma vulnerabilidade com sucesso teve acesso a dados confidenciais. (Tabela 2.5)

2. ”Impacto na integridade” (*Integrity Impact*): Na medida em que o atacante ao explorar uma vulnerabilidade com sucesso modificou dados ou ficheiros. (Tabela 2.6)

3. ”Impacto na disponibilidade” (*Availability Impact*): Na medida em que o atacante ao explorar uma vulnerabilidade com sucesso impossibilita o acesso a serviços ou recursos do componente impactado. (Tabela 2.7)

Opção	Valor	String
Alto (*High*)	0.56	H
Baixo (*Low*)	0.22	L
Nenhum (*None*)	0	N

Tabela 2.5: ”Métrica Base” (*Base Metric*) - ”Impacto na Confidencialidade” (*Confidentiality Impact*) [8]

Opção	Valor	String
Alto (*High*)	0.56	H
Baixo (*Low*)	0.22	L
Nenhum (*None*)	0	N

Tabela 2.6: ”Métrica Base” (*Base Metric*) - ”Impacto na Integridade” (*Integrity Impact*) [8]

Opção	Valor	String
Alto (*High*)	0.56	H
Baixo (*Low*)	0.22	L
Nenhum (*None*)	0	N

Tabela 2.7: ”Métrica Base” (*Base Metric*) - ”Impacto na Disponibilidade” (*Availability Impact*) [8]

O ”âmbito” (*scope*), fator inserido na versão 3 do CVSS, também incluído na ”métrica base” (*base metric*), possibilita diferenciar vulnerabilidades em que o impacto recai sobre o componente vulnerável ou sobre um componente distinto, denominado por componente impactado. Por exemplo, para que seja explorada uma vulnerabilidade do tipo *Cross Site Scripting (XSS)*, é necessário ultrapassar os mecanismos e propriedades de segurança do servidor web para injetar código malicioso na aplicação, no entanto o impacto causado na exploração dessa vulnerabilidade recai sobre o cliente e não sobre o servidor, visto que este código só é executado no browser do cliente e consequentemente vai afetar o computador do mesmo. Como é possível verificar na Figura 2.1, se o valor do ”âmbito” (*scope*) for ”alterado” (*Scope Changed*) influencia o *sub score* do impacto e também o resultado final da ”métrica base” (*base metric*). Para além disso, o valor dos ”privilégios requeridos” (*Privilege Required*) também aumenta à medida que os privilégios são mais elevados (Tabela 2.3).

Base Score	
If (Impact Sub score =< 0)	*0 Else,*
Scope Unchanged	$RoundUp_1\ (Minimum\ [(Impact + Exploitability), 10])$
Scope Changed	$RoundUp_1\ (Minimum\ [1.08 \times (Impact + Exploitability), 10])$

Impact Sub score	
Scope Unchanged	$6.42 \times ISC_{Base}$
Scope Changed	$7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

Where $ISC_{Base} = 1 - [(1 - Impact_{conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$

Exploitability Sub score
$8.22 \times Attack\ Vector \times Attack\ Complexity \times Privilege\ Required \times User\ Interaction$

Figura 2.1: Equações da ”métrica base”(*base metric*) do CVSS v3, extraído de [9]

O ”Grupo da Métrica Temporal” (*Temporal Metric Group*) é constituído pelos seguintes três fatores, que determinam as características da vulnerabilidade, tendo em considera-

ção o estado atual das técnicas de exploração, a existência de *patches* ou *workaround*, e o grau de confiança das fontes:

1. ”Maturidade do código de exploração” (*Exploit Code Maturity*): Mede o estado atual das técnicas de exploração ou código disponível. (Tabela 2.8)

2. ”Nível de remediação” (*Remediation level*): Mede o nível de eficiência na mitigação da vulnerabilidade, considerando a disponibilização de uma solução temporária ou definitiva. (Tabela 2.9)

3. ”Grau de confiança” (*Report Confidence*): Credibilidade na fonte que publicou a vulnerabilidade e nos detalhes técnicos conhecidos. (Tabela 2.10)

Opção	Valor	String
Não definido (*Not defined*)	1	X
Alto (*High*)	1	H
Funcional (*Functional*)	0.97	F
Prova de conceito (*Proof of concept*)	0.94	P
Não provado (*Unproven*)	0.91	U

Tabela 2.8: ”Métrica Temporal” (*Temporal Metric*) – Maturidade do código de exploração (*Exploit Code Maturity*) [8]

Opção	Valor	String
Não definido (*Not defined*)	1	X
Indisponível (*Unavailable*)	1	U
Solução alternativa (*Workaround*)	0.97	W
Correção temporária (*Temporary Fix*)	0.96	T
Correção oficial (*Official Fix*)	0.95	O

Tabela 2.9: ”Métrica Temporal” (*Temporal Metric*) - Nível de remediação (*Remediation level*) [8]

Opção	Valor	String
Não definido (*Not defined*)	1	X
Confirmado (*Confirmed*)	1	C
Razoável (*Reasonable*)	0.96	R
Desconhecido (*Unknown*)	0.92	U

Tabela 2.10: ”Métrica Temporal” (*Temporal Metric*) - Grau de confiança (*Report Confidence*) [8]

O *score* da ”métrica temporal” (*temporal metric*) é definido pelo produto dos três fatores mencionados anteriormente com o valor obtido da ”métrica base” (*base metric*) (Figura 2.2).

Temporal Score

$$RoundUp_1(Base\ Score \times Exploitability_{Temporal} \times Remediation\ Level \times Report\ Confidence)$$

Figura 2.2: Equações da ”métrica temporal” (*temporal metric*) do CVSS v3, extraído de [9]

O ”Grupo da Métrica Ambiental” (*Environmental Metric Group*) é constituído por onze fatores, que representam a importância do ativo na organização considerando os requisitos na confidencialidade, integridade e disponibilidade e os mecanismos de segurança implementados no ambiente onde o ativo se insere. Como tal, são divididos nos dois grupos de métricas seguintes:

1. ”Requisitos de segurança” (*Security Requirements*): Influencia o valor da submétrica impacto da métrica base, pois é considerada a relevância do ativo em cada uma das propriedades de segurança mencionadas. (Tabela 2.11, 2.12 e 2.13)

2. ”Modificação da Métrica Base” (*Modified Base Metric*): Influencia o valor da submétrica exploração da métrica base, pois os mecanismos de segurança aplicados ao ambiente em que o ativo está inserido pode dificultar ou facilitar a vida do atacante na exploração da vulnerabilidade. (Tabelas 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 e 2.7)

Opção	Valor	String
Não definido (*Not Defined*)	1	X
Alto (*High*)	1.5	H
Médio (*Medium*)	1.0	M
Baixo (*Low*)	0.5	L

Tabela 2.11: ”Métrica Ambiental” (*Environmental Metric*) - ”Requisitos na confidencialidade” (*Confidentiality Requirement*) [8]

Opção	Valor	String
Não definido (*Not Defined*)	1	X
Alto (*High*)	1.5	H
Médio (*Medium*)	1.0	M
Baixo (*Low*)	0.5	L

Tabela 2.12: ”Métrica Ambiental” (*Environmental Metric*) - ”Requisitos na integridade” (*Integrity Requirement*) [8]

Opção	Valor	String
Não definido (*Not Defined*)	1	X
Alto (*High*)	1.5	H
Médio (*Medium*)	1.0	M
Baixo (*Low*)	0.5	L

Tabela 2.13: ”Métrica Ambiental” (*Environmental Metric*) - ”Requisitos na disponibilidade” (*Availability Requirement*) [8]

Os cálculos para determinar o *score* do ”Grupo da Métrica Ambiental” (*Environmental Metric Group*) são semelhantes à métrica base (*base metric*), com o acréscimo dos respetivos fatores desta métrica (Figura 2.3).

Environmental Score	
If (Modified Impact Sub score =< 0)	*0 Else,*
Modified Scope Unchanged	$RoundUp_1(Minimum\,[(M.Impact + M.Exploitability) \times Exploitability_{Temporal} \times Remediation\ Level \times Report\ Confidence, 10])$
Modified Scope Changed	$RoundUp_1\,(Minimum\,[1.08 \times (M.Impact + M.Exploitability) \times Exploitability_{Temporal} \times Remediation\ Level \times Report\ Confidence, 10])$

Modified Impact Sub score	
Modified Scope Unchanged	$6.42 \times [ISC_{Modified}]$
Modified Scope Changed	$7.52 \times [ISC_{Modified} - 0.029]$-$3.25 \times [ISC_{Modified} - 0.02]^{15}$

Where $ISC_{Modified} = Minimum\,[1 - (1 - M.I_{conf} \times CR) \times (1 - M.I_{Integ} \times IR) \times (1 - M.I_{Avail} \times AR)], 0.915]$

Modified Exploitability Sub score
$8.22 \times M.Attack\ Vector \times M.Attack\ Complexity \times M.Privilege\ Required \times M.User\ Interaction$

Figura 2.3: Equações da ”métrica ambiental” (*environmental metric*) do CVSS v3, extraído de [9]

A fórmula final depende da informação disponibilizada relativamente à vulnerabilidade que vai ser avaliada, dado que se apenas forem conhecidos os fatores obrigatórios da métrica base, então a fórmula final encontra-se na Figura 2.1, se adicionalmente forem

conhecidos os valores da métrica temporal então a fórmula final encontra-se na Figura 2.2, e por último, se existirem informações referentes ao ativo na organização então a fórmula final encontra-se na Figura 2.3.

Para além do método quantitativo, foi introduzido nesta versão o método qualitativo, em que a sua utilização é opcional e apenas serve para apoiar as organizações na gestão de vulnerabilidades. A escala dos valores quantitativos é de 0.0 a 10.0, que contabiliza um total de 101 valores. Estes valores podem ser correspondidos no respetivo valor qualitativo, como ilustrado na Tabela 2.14.

Valor Qualitativo	Valor Quantitativo
Nenhum (*None*)	0.0
Baixo (*Low*)	0.1 - 3.9
Médio (*Medium*)	4.0 - 6.9
Alto (*High*)	7.0 - 8.9
Crítico (*Critical*)	9.0 - 10.0

Tabela 2.14: Mapeamento dos valores quantitativos em qualitativos [8]

Após o preenchimento e cálculo das métricas obtém-se uma representação textual denominada por *Vector String*, que representa o conjunto de valores escolhidos para o cálculo do *score* da respetiva vulnerabilidade (Tabela 2.15).

Métrica	Nome da Métrica e Nome Abreviado	Valores Possíveis
Base (*Base*)	Superfície de Ataque (*Attack Vector*), AV	[N,A,L,P]
	Complexidade do Ataque (*Attack Complexity*), AC	[L,H]
	Privilégios Requeridos (*Privilege Required*), PR	[N,L,H]
	Interação do utilizador (*User Interaction*), UI	[N,R]
	Âmbito (*Scope*), S	[U,C]
	Impacto na Confidencialidade (*Confidentiality Impact*), C	[H,L,N]
	Impacto na Integridade (*Integrity Impact*), I	[H,L,N]
	Impacto na Disponibilidade (*Availability Impact*), A	[H,L,N]
Temporal (*Temporal*)	Maturidade do Código de Exploração (*Exploit Code Maturity*), E	[X,H,F,P,U]
	Nível de Remediação (*Remediation Level*), RL	[X,U,W,T,O]
	Grau de Confiança (*Report Confidence*), RC	[X,C,R,U]
Ambiental (*Environmental*)	Requisitos na Confidencialidade (*Confidentiality Requirements*), CR	[X,H,M,L]
	Requisitos na Integridade (*Integrity Requirements*), IR	[X,H,M,L]
	Requisitos na Disponibilidade (*Availability Requirements*), AR	[X,H,M,L]
	Alteração da Superfície de Ataque (*Modified Attack Vector*), MAV	[X,N,A,L,P]
	Alteração da Complexidade do Ataque (*Modified Attack Complexity*), MAC	[X,L,H]
	Alteração dos Privilégios Requeridos (*Modified Privilege Required*), MPR	[X,N,L,H]
	Alteração da Interação do Utilizador (*Modified User Interaction*), MUI	[X,N,R]
	Alteração do Âmbito (*Modified Scope*), MS	[X,U,C]
	Alteração do Impacto na Confidencialidade (*Modified Confidentiality Impact*), MC	[X,N,L,H]
	Alteração do Impacto na Integridade (*Modified Integrity Impact*), MI	[X,N,L,H]
	Alteração do Impacto na Disponibilidade (*Modified Availability Impact*), MA	[X,N,L,H]

Tabela 2.15: Representação textual de cada grupo de métricas, extraído de [8]

2.2 WIVSS – Weighted Impact Vulnerability Scoring System

Como já foi referido no início deste capítulo, foram propostas várias metodologias com o objetivo de melhorar o CVSSv2, uma delas é o WVISS [46]. O propósito desta metodologia consiste em aumentar a fiabilidade dos *scores* e diversificar os mesmos. Apenas é considerada a métrica base do CVSSv2, visto que esta é a única obrigatória para o cálculo da severidade de cada vulnerabilidade.

Como foi mencionado em vários trabalhos relacionados ([17], [45], [46], [47]), o impacto na confidencialidade é considerado o mais severo, pois muito dificilmente é identificado o roubo/furto de informação confidencial e normalmente só é descoberto após publicamente exposto. O impacto na integridade é o segundo mais severo considerando que normalmente uma alteração sobre uma determinada informação resulta na indisponibilidade de um serviço. Como indicado, a disponibilidade é facilmente recuperável enquanto que relativamente à confidencialidade não há forma de recuperar a informação furtada. O mesmo se aplica à integridade, pois a complexidade na identificação da violação, alteração e recuperação é bastante maior do que a identificação da indisponibilidade de um serviço e recuperação do mesmo.

Pelos motivos indicados anteriormente, os autores mantiveram os valores da sub-métrica exploração e alteraram os valores da sub-métrica impacto (Tabela 2.16 e Tabela 2.17). Estes valores são baseados em aproximações matemáticas que garantem a heterogeneidade de valores e reflete a severidade da vulnerabilidade.

Fatores da métrica	Valor da métrica	Valor numérico
Superfície de ataque (*Attack Vector*)	Local, Adjacente à rede, Rede (*Local*, *Adjacent Network*, *Network*)	0.395, 0.646, 1
Complexidade do ataque (*Attack Complexity*)	Alto, Médio, Baixo (*High*, *Medium*, *Low*)	0.35, 0.61, 0.71
Autenticação (*Authentication*)	Múltipla, Singular, Nenhuma (*Multiple*, *Single*, *None*)	0.45, 0.56, 0.704
Impacto na Confidencialidade (*Confidentiality Impact*)	Nenhum, Parcial, Total (*None*, *Partial*, *Complete*)	0.0, 0.275, 0.660
Impacto na Integridade (*Integrity Impact*)	Nenhum, Parcial, Total (*None*, *Partial*, *Complete*)	0.0, 0.275, 0.660
Impacto na Disponibilidade (*Availability Impact*)	Nenhum, Parcial, Total (*None*, *Partial*, *Complete*)	0.0, 0.275, 0.660

Tabela 2.16: Os *scores* definidos na métrica base (*base metric*) no CVSS v2 [46]

Como já referido anteriormente, as fórmulas do CVSSv2 são baseadas em aproximações matemáticas e foram criadas com a perícia e conhecimento dos elementos do CVSS-SIG [46]. As fórmulas do WIVSS são também baseadas em aproximações matemáticas

Fatores da métrica	Valor da métrica	Valor numérico
Superfície de ataque (*Attack Vector*)	Local, Adjacente à rede, Rede (*Local*, *Adjacent Network*, *Network*)	0.395, 0.646, 1
Complexidade do ataque (*Attack Complexity*)	Alto, Médio, Baixo (*High*, *Medium*, *Low*)	0.35, 0.61, 0.71
Autenticação (*Authentication*)	Múltipla, Singular, Nenhuma (*Multiple*, *Single*, *None*)	0.45, 0.56, 0.704
Impacto na Confidencialidade (*Confidentiality Impact*)	Nenhum, Parcial, Total (*None*, *Partial*, *Complete*)	0.0, 1.5, 3.0
Impacto na Integridade (*Integrity Impact*)	Nenhum, Parcial, Total (*None*, *Partial*, *Complete*)	0.0, 1.2, 2.4
Impacto na Disponibilidade (*Availability Impact*)	Nenhum, Parcial, Total (*None*, *Partial*, *Complete*)	0.0, 0.8, 1.6

Tabela 2.17: Os *scores* definidos na métrica base (*base metric*) no WIVSS [46]

e como suporte às mesmas foram consideradas as seguintes regras relativas à sub-métrica de impacto:

- O impacto na confidencialidade é maior do que o impacto na integridade e disponibilidade, e o impacto na integridade é maior que o impacto na disponibilidade;
- O impacto é igual a 0, se a exploração da vulnerabilidade não tiver qualquer impacto;
- O valor relativo à opção parcial é metade da opção total, assim como o valor relativo à opção total é o dobro da opção parcial;
- A pontuação está entre 0.0 e 7.0 inclusive;
- A soma total das vinte e sete combinações possíveis têm de ser diferentes.

Relativamente às fórmulas das duas metodologias, estas diferem tanto no cálculo da sub-métrica de impacto como nas restantes fórmulas, como é possível verificar abaixo:

Pontuacao do WIVSS = arredondado a um decimal (Pontuacao da Exploracao + Pontuacao do Impacto) * f(impacto)

Pontuacao do Impacto = Impacto na Confidencialidade + Impacto na Integridade + Impacto na Disponibilidade

Pontuacao na Exploracao = 6 * Superficie de ataque * Complexidade do ataque * Autenticacao

Pontuacao do CVSSv2 = arredondado a um decimal (((0.6 * Pontuacao do Impacto) + (0.4 * Pontuacao na Exploracao) - 1.5) * f(Impact))

Pontuacao do Impacto = 10.41 * (1 - (1 - Impacto na Confidencialidade) * (1-Impacto na Integridade) * (1 - Impacto na disponibilidade))

Pontuacao na Exploracao = 20 * Superficie de ataque * Complexidade do ataque * Autenticacao

Com base nas fórmulas acima referenciadas, é possível inferir que a sub-métrica de impacto do WIVSS pesa 70% do resultado final, enquanto que no CVSSv2 pesa 60% e como tal a sub-métrica de exploração vale mais 10% no CVSSv2 que no WVISS, 40% e 30% respetivamente.

A pontuação do impacto é igual a 0 se o f(impacto) também for igual a 0, caso contrário é igual a 1. Já no CVSSv2 se a pontuação do impacto for diferente de 0 então o f(impacto) é igual a 1.176.

Como trabalho futuro, os autores propuseram a criação de um algoritmo baseado em regras que refletisse o impacto real das vulnerabilidades em sistemas de informação.

No CVSS versão 1, esta proposta de melhoria ao CVSSv2 não foi aprovada pelo comité do CVSS-SIG [45], e os mesmos autores do WIVSS propuseram a melhoria anteriormente indicada a esta metodologia.

No WIVSS versão 2, foram criadas as duas seguintes regras para além das cinco já existentes:

- O impacto total na integridade é maior que o impacto parcial na confidencialidade;
- O impacto total na disponibilidade é maior que o impacto parcial na integridade.

Enquanto no WIVSS versão 1, os pesos da sub-métrica impacto foram derivados heuristicamente através de tentativa erro, o que não oferece segurança e certeza se estes valores são os melhores relativamente à diversidade [45], o objetivo na versão 2 foi encontrar valores melhores para os impactos na confidencialidade, integridade e disponibilidade. Desta forma, definiram um algoritmo de pesquisa (Figura 2.4) para calcular todas as combinações possíveis considerando as sete regras definidas e obtiveram quatorze combinações diferentes. Calcularam a distribuição de valores tanto para o CVSSv2 como para as quatorze combinações diferentes do WIVSS, com uma amostragem de 20,496 vulnerabilidades existentes no NVD [24], em que foi calculado o mínimo, máximo, média, desvio padrão, 1/4 e 3/4 quartis, coeficiente de variação e número de diferentes *scores* (Figura 2.5), com o propósito de compararem estas estatísticas com as do CVSSv2 e identificarem a combinação ótima do WIVSS que contribua para a diversificação e fiabilidade de valores.

Start

$W_{Availability} = 1.2$

Step = 0.2

While $W_{Availability} <= 2$

    $W_{Integrity} = W_{Availability} + Step$

    $W_{Confidentiality} = 7 - (W_{Integrity} + W_{Availability})$

    While $W_{Integrity} < W_{Confidentiality}$

        If $2 * W_{Availability} > W_{Integrity}$ AND $2 * W_{Integrity} > W_{Confidentiality}$

            Compute the 3^3 Possible Sums for this Combination of Weights

            If the 3^3 Possible Sums have different values

                Save this Combination of Weights

            EndIf

        EndIf

        $W_{Integrity} = W_{Integrity} + Step$

        $W_{Confidentiality} = W_{Confidentiality} - Step$

    EndWhile

    $W_{Availability} = W_{Availability} + Step$

EndWhile

Output of the algorithm: the Final Combinations of Weights

End

Figura 2.4: Algoritmo WIVSSv2, extraído de [45]

Após análise dos valores apresentados na Figura 2.5 escolheram a 2ª opção (WIVSS2) pois a distribuição de valores é maior comparativamente ao CVSSv2 e às restantes combinações. Para além disso, a média é menor no WIVSS2 do que no CVSSv2, 6.42 e 6.9 respetivamente, como também a mediana, 5.91 e 5.9 respetivamente. Estas estatísticas indicam que o CVSSv2 pontua as vulnerabilidades com valores demasiado elevados [45]. Desta forma, os novos valores propostos para a sub-métrica de impacto estão apresentados na Tabela 2.18.

Os autores evidenciaram que a diversidade é maior no WIVSS versão 2 através da comparação de três vulnerabilidades que no CVSSv2 continham o mesmo *score* (7.8)

Name	Mean	Min	25%	Median	75%	Max	St. Deviation	Coefficient of Variation	Different Scores
CVSS	**6.42**	**0**	**4.3**	**6.9**	**7.5**	**10**	**2.17**	**0.338**	**69**
WIVSS1	5.91	0	3.6	5.9	8	10	2.44	0.412	75
WIVSS2	**5.91**	**0**	**3.7**	**5.9**	**8**	**10**	**2.43**	**0.411**	**76**
WIVSS3	5.91	0	3.7	5.8	8	10	2.43	0.411	75
WIVSS4	5.92	0	3.7	5.8	8	10	2.41	0.407	74
WIVSS5	5.92	0	3.8	5.8	8	10	2.40	0.405	75
WIVSS6	5.93	0	3.9	5.7	8	10	2.40	0.405	72
WIVSS7	5.92	0	3.7	5.7	8	10	2.41	0.407	74
WIVSS8	5.93	0	3.8	5.7	8	10	2.39	0.403	73
WIVSS9	5.93	0	3.9	5.7	8	10	2.39	0.403	71
WIVSS10	5.92	0	3.7	5.6	8	10	2.41	0.407	73
WIVSS11	5.93	0	3.7	5.6	8	10	2.40	0.405	73
WIVSS12	5.93	0	3.8	5.6	8	10	2.39	0.403	75
WIVSS13	5.93	0	3.7	5.5	8	10	2.39	0.403	69
WIVSS14	5.94	0	3.8	5.5	8	10	2.38	0.400	74

Figura 2.5: Estatísticas e distribuição de valores WIVSSv2, extraído de [45]

Nome da métrica	Valor da métrica	Peso da métrica
Impacto na Confidencialidade	Nenhum, Parcial, Total	0.0, 1.8, 3.6
Impacto na Integridade	Nenhum, Parcial, Total	0.0, 1.1, 2.2
Impacto na Disponibilidade	Nenhum, Parcial, Total	0.0, 0.6, 1.2

Tabela 2.18: Os valores escolhidos para a sub-métrica de impacto da métrica base (*base metric*) do WIVSSv2 [45]

e no WIVSSv2 continham diferentes *scores*, com valores menores e distantes uns dos outros (4.2, 5.2 e 6.6). Assim, comprovaram que a combinação de valores escolhida melhora a diversidade e fiabilidade dos valores, pois considera o impacto de cada vulnerabilidade e consoante a severidade do impacto atribui o peso correspondente. Além do mais, na amostragem referida verificou-se mais valores heterogéneos e a média desses valores encontra-se mais perto do valor médio da escala de 0 a 10, o que significa que tem menos vulnerabilidades com pontuação elevada [45].

2.3 VRSS – Vulnerability Rating and Scoring System

À semelhança do WIVSS, a metodologia *Vulnerability Rating and Scoring Systems (VRSS)* também pretende melhorar o CVSSv2. O propósito desta metodologia consiste em atribuir valores qualitativos e quantitativos a cada vulnerabilidade [13]. O objetivo é agrupar as vulnerabilidades em níveis de severidade considerando os impactos do CVSSv2 como melhoria. Desta forma, visam separar as vulnerabilidades o máximo possível consoante o seu impacto, e posteriormente pontuá-las considerando os mesmos fatores na sub-métrica de exploração da métrica base do CVSSv2. Atribuíram assim ainda mais peso à sub-métrica de impacto e consequentemente diminuíram o peso à sub-métrica de exploração, com 90% e 10% respetivamente.

Como primeira abordagem, qualificaram as vinte e sete combinações possíveis da sub-métrica de impacto conforme o nível de risco e posteriormente quantificaram cada combinação considerando o mapeamento realizado entre os níveis de severidade e as pontuações separadas entre intervalos por cada nível (Figura 2.6 e Figura 2.7 respetivamente). A Figura 2.8 ilustra o sistema de avaliação desenvolvido para a avaliação de vulnerabilidades considerando os dois métodos qualitativo e quantitativo já mencionados anteriormente.

ID	Description	Possible impact metrics cases	Qualitative level	Impact score
1	Each of confidentiality, integrity, and availability properties has a "complete" loss	[C:C/I:C/A:C]	High	9
2	One of confidentiality, integrity, and availability properties has a "partial" loss. The other two have a "complete" loss	[C:P/I:C/A:C], [C:C/I:P/A:C], [C:C/I:C/A:P]	High	8
3	One of confidentiality, integrity, and availability properties has a "none" loss. The other two have a "complete" loss	[C:N/I:C/A:C], [C:C/I:N/A:C], [C:C/I:C/A:N]	High	7
4	One of confidentiality, integrity, and availability properties has a "complete" loss. The other two have a "partial" loss	[C:C/I:P/A:P], [C:P/I:C/A:P], [C:P/I:P/A:C]	High	6
5	One of confidentiality, integrity, and availability properties has a "complete" loss. One of them has a "partial" loss, and one has a "none" loss	[C:C/I:P/A:N], [C:C/I:N/A:P], [C:P/I:C/A:N], [C:P/I:N/A:C], [C:N/I:C/A:P], [C:N/I:P/A:C]	Medium	5
6	One of confidentiality, integrity, and availability properties has a "complete" loss. The other two have a "none" loss	[C:C/I:N/A:N], [C:N/I:C/A:N], [C:N/I:N/A:C]	Medium	4
7	Each of confidentiality, integrity, and availability properties has a "partial" loss	[C:P/I:P/A:P]	Medium	3
8	One of confidentiality, integrity, and availability properties has a "none" loss. The other two have a "partial" loss	[C:N/I:P/A:P], [C:P/I:N/A:P], [C:P/I:P/A:N]	Medium	2
9	One of confidentiality, integrity, and availability properties has a "partial" loss. The other two have a "none" loss	[C:P/I:N/A:N], [C:N/I:P/A:N], [C:N/I:N/A:P]	Low	1
10	Each of confidentiality, integrity, and availability properties has a "none" loss	[C:N/I:N/A:N]	Low	0

Figura 2.6: VRSS - Qualitativa e Quantitativa, extraído de [13]

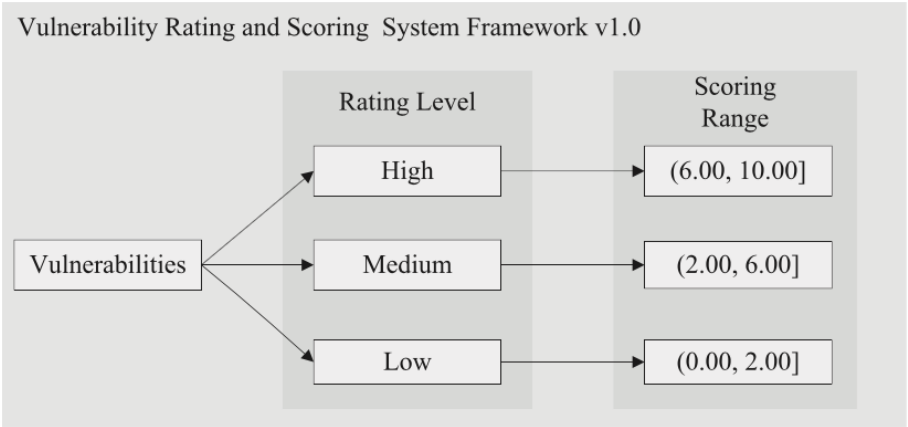

Figura 2.7: VRSS - Mapeamento do modelo qualitativo para o quantitativo, extraído de [13]

Após a classificação e pontuação da sub-métrica de impacto é realizada a soma entre o impacto e a exploração. Dado que os valores da sub-métrica exploração são idênticos aos do CVSSv2, a diferença advém da atribuição de um peso inferior a esta sub-métrica. As fórmulas que suportam o valor quantitativo encontram-se de seguida:

$$\textbf{Pontuacao Quantitativa} = \text{Pontuacao\_impacto} + \text{Pontuacao\_exploracao} \tag{2.1}$$

Pontuacao_exploracao = 2 * Superficie_de_ataque * Complexidade_do_ataque * Autenticacao (2.2)

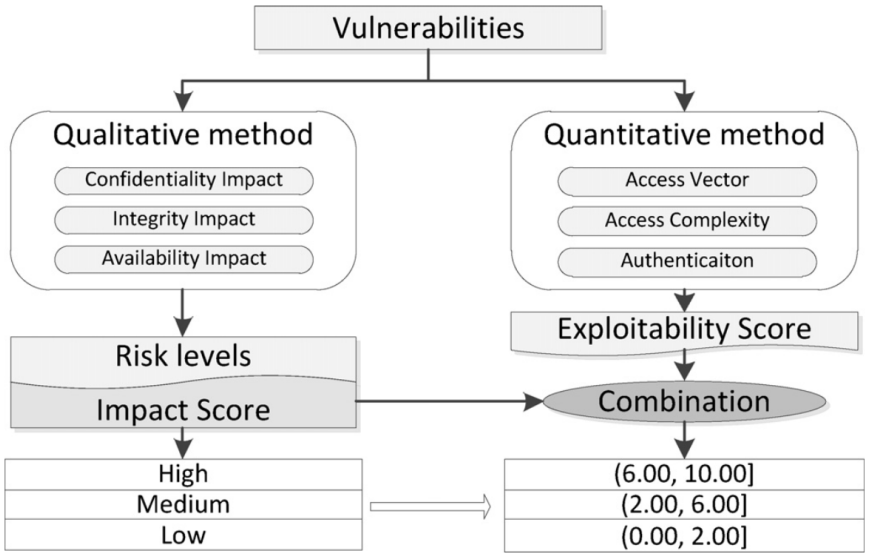

Figura 2.8: VRSS - Sistema de avaliação de vulnerabilidades, extraído de [14]

Relativamente aos resultados, os autores consideraram que os objetivos foram atingidos, visto terem diminuído o número de vulnerabilidades com grau de severidade elevado e consequentemente o número de vulnerabilidades com valor médio aumentaram. Como indicado pelos autores, é expetável existir mais vulnerabilidades com grau de severidade médio do que com alto ou baixo. Para além disso, alcançaram o objetivo principal, dado que distanciaram as vulnerabilidades com *scores* distintos, de acordo com a severidade do impacto de cada vulnerabilidade.

Esta metodologia foi melhorada, com o contributo de mais dois elementos para além dos autores da primeira versão, dado que as vulnerabilidades não foram suficientemente separadas [14]. Com o propósito de aumentar a diversidade dos resultados, os autores decidiram introduzir uma nova variável denominada por tipo de vulnerabilidade - *vulnerability type factor (VTF)*, com a finalidade de distinguir melhor as vulnerabilidades umas das outras.

Com a introdução deste novo fator à fórmula (2.3), foi diminuído o peso da submétrica de exploração (2.4) da métrica base, ou seja, em vez de 10% foi atribuído apenas 2% e os restantes 8% ao tipo de vulnerabilidade. Deste modo, o impacto é qualificado para avaliar o risco associado, a exploração e o tipo de vulnerabilidade que são utilizados para diferenciar as vulnerabilidades com o mesmo impacto. Este novo fator foi

incorporado à *framework* desenvolvida na versão 1 do VRSS (Figura 2.9) e com base na taxonomia disponibilizada pelo *Common Weakness Enumeration (CWE)* [21], separaram as vulnerabilidades pelos identificadores do CWE e respetivo tipo.

Pontuacao Quantitativa = Pontuacao_impacto + VTF + Pontuacao_exploracao (2.3)

Pontuacao_exploracao = Superficie_de_ataque * Complexidade_do_ataque * Autenticacao (2.4)

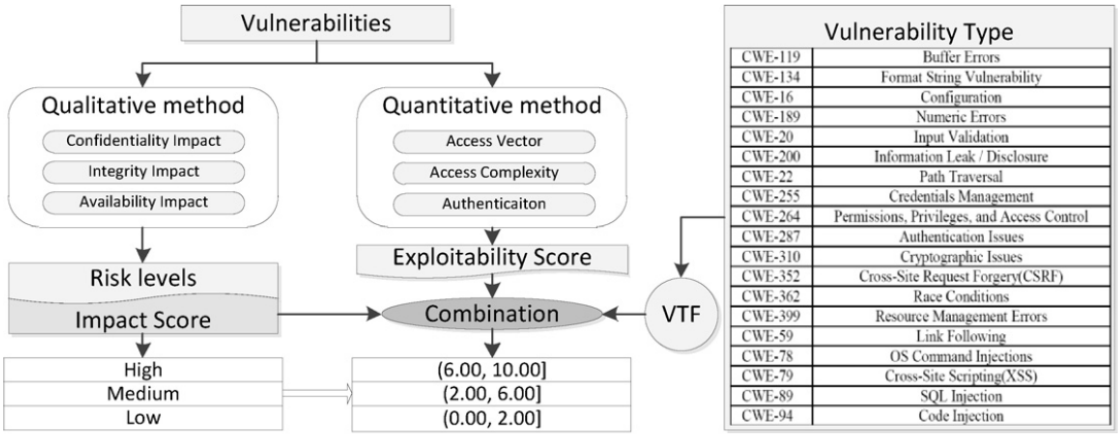

Fig. 8. Improving VRSS using vulnerability type.

Figura 2.9: VRSS - Framework v2, extraído de [14]

Os autores consideraram dezanove tipos de vulnerabilidades e aplicaram o processo analítico hierárquico (*Analytic Hierarchy Process - AHP*), que é um método que utiliza uma estrutura hierárquica para decompor um problema complexo em vários pequenos sub-problemas e tem sido bastante utilizado para espelhar a importância dos fatores associados à severidade [14]. Como abordagem, consideraram os níveis de risco alto, médio e baixo para calcularem os pesos correspondentes a cada tipo de vulnerabilidade. Utilizando o *AHP* e a abordagem referida anteriormente, foram encontrados os valores para cada tipo de vulnerabilidade (Tabela 2.19).

Os resultados foram bastante positivos, uma vez que obtiveram muito mais diversidade de valores que o CVSSv2 e o VRSSv1, 57 e 97 respetivamente, para 274 nesta nova versão do VRSS. Deste modo, evidenciaram que a utilização do ”Tipo de vulnerabilidade” (*Vulnerability Type*) ajuda as organizações a priorizar mais facilmente as vulnerabilidades identificadas nos seus ativos.

ID	CWE-ID	Tipo de vulnerabilidade	VTF
C1	CWE-119	*Buffer errors*	1.71
C2	CWE-134	*Format string vulnerability*	1.18
C3	CWE-16	*Configuration*	1.02
C4	CWE-189	*Numeric errors*	1.31
C5	CWE-20	*Input validation*	1.07
C6	CWE-200	*Information leak/disclosure*	1.01
C7	CWE-22	*Path transversal*	1.02
C8	CWE-255	*Credentials management*	1.07
C9	CWE-264	*Permissions, privileges, and access control*	1.07
C10	CWE-287	*Authentication issues*	1.06
C11	CWE-310	*Cryptographic issues*	1
C12	CWE-352	*Cross-site Request Forgery (CSRF)*	1.09
C13	CWE-362	*Race conditions*	1.16
C14	CWE-399	*Resource management erros*	1.12
C15	CWE-59	*Link following*	1.48
C16	CWE-78	*OS Command Injections*	2
C17	CWE-79	*Cross-site scripting (XSS)*	1.09
C18	CWE-89	*SQL injection*	1.15
C19	CWE-94	*Code injection*	1.34

Tabela 2.19: AHP - Valores encontrados para cada tipo de vulnerabilidade (VTF) considerado

2.4 OWASP – Risk Rating Methodology

O Open Web Application Security Project (OWASP) é uma organização, sem fins lucrativos e de reconhecimento internacional, que contribui para a melhoria da segurança aplicacional e ajuda as organizações a tomar decisões informadas acerca dos riscos associados às vulnerabilidades existentes [28]. Nesta organização são desenvolvidos desde conteúdos, ferramentas, fóruns com a participação de diversos elementos de organizações como a Qualys, Adobe, Fortify, Fortinet e Rapid7 [30].

A lista OWASP Top 10 apresenta as vulnerabilidades aplicacionais mais críticas (Figura 2.10) e tem como propósito instruir os programadores, desenhistas, arquitetos, gestores e organizações relativamente ao impacto destas vulnerabilidades. Esta lista foi desenvolvida através de vários elementos especializados em segurança aplicacional e foi baseada em oito bases de dados de sete organizações especializadas em segurança aplicacional, incluindo quatro empresas de consultoria e três aplicações de fornecedores (1 estático, 1 dinâmico, e um para ambos). Estes dados englobam mais de 500 mil vulnerabilidades em centenas de organizações e milhares de aplicações [32].

O OWASP desenvolveu vários conteúdos relevantes para a segurança aplicacional, entre os quais uma metodologia para calcular o risco de cada vulnerabilidade existente

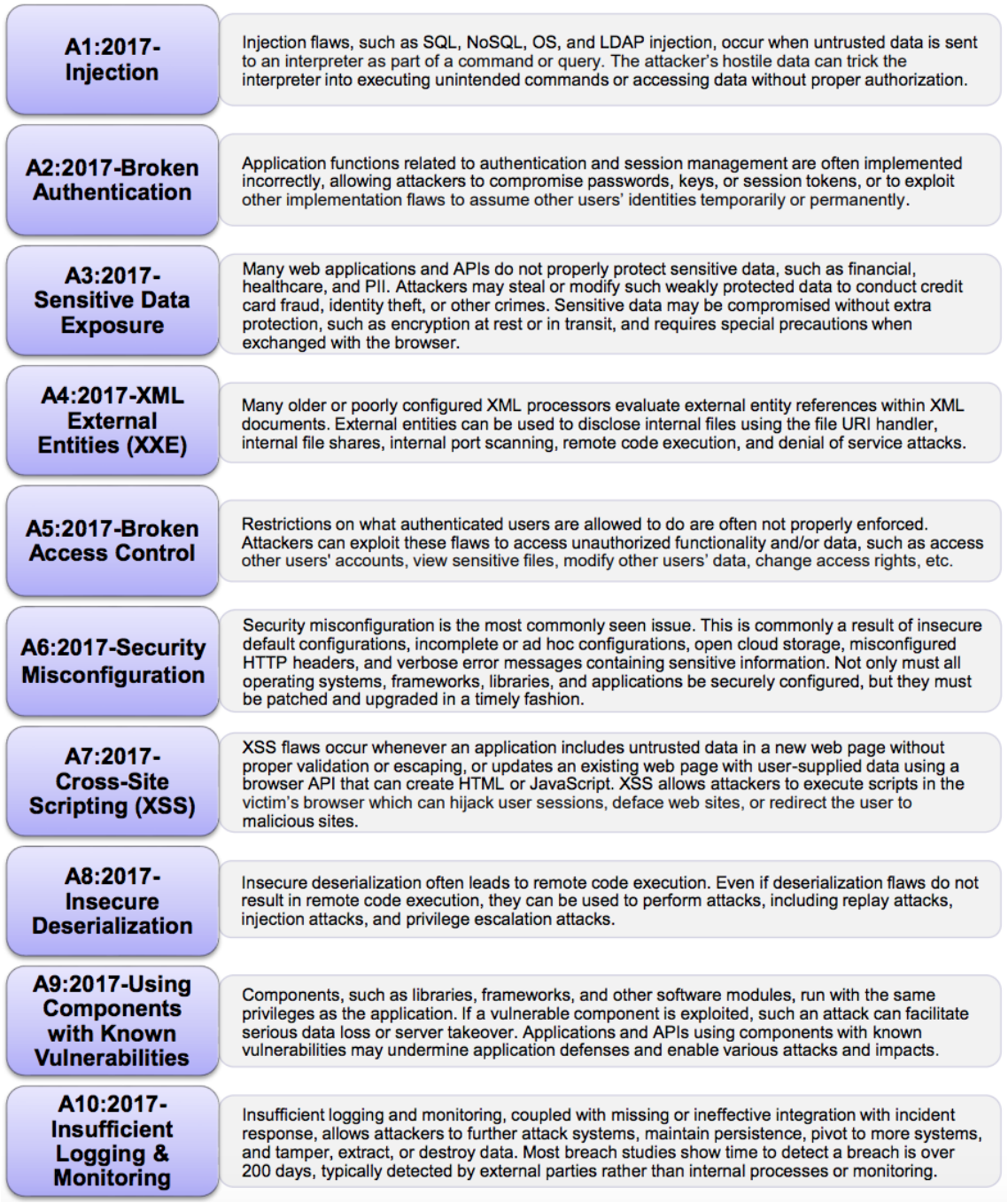

Figura 2.10: Top 10 das vulnerabilidades mais severas, extraído de [32]

nas organizações, denominada por *"The OWASP Risk Rating Methodology"* [31]. Como mencionado pelos autores, esta é uma metodologia base que deve ser customizada particularmente para cada organização.

A abordagem que utilizaram é baseada nas metodologias mais conhecidas, como o CVSS, e customizada para a segurança aplicacional. Foi considerado o modelo padrão de

risco (Fórmula 2.5) como ponto de partida e determinados os passos para calcular o risco.

$$Risco = Verosimilhança * Impacto \tag{2.5}$$

O primeiro passo é a identificação dos possíveis riscos existentes nos ativos de informação ou processos de negócio. Como tal é necessário reunir toda a informação associada a possíveis ameaças e ataques, às vulnerabilidades identificadas, bem como o impacto no negócio de uma exploração bem-sucedida. Podem existir diversos grupos de possíveis atacantes, ou até mesmo múltiplos impactos no negócio mas como os autores indicam, é sempre melhor considerar o pior caso pois assim é determinado o maior risco possível para o caso em estudo.

Posteriormente, deve ser estimada a probabilidade de explorar os riscos identificados. Desta forma, o segundo passo é identificar e caraterizar os fatores que suportam o cálculo do primeiro indicador da fórmula, a "verosimilhança" (*likelihood*). Para calcular a verosimilhança de existir um ataque bem-sucedido por um grupo de atacantes é necessário estimar o nível de perícia, a motivação, a oportunidade e a dimensão do grupo. Já para calcular a verosimilhança de uma vulnerabilidade em particular ser descoberta e explorada é preciso estimar a facilidade na identificação, a facilidade na exploração, o conhecimento e deteção da intrusão. Deste modo, é apresentado de seguida em mais detalhe as questões que têm de ser colocadas para determinar a opção mais indicada para cada fator/variável:

1. Fatores inerentes à ameaça
    (a) Nível de perícia – Qual o nível de perícia técnica? (Tabela 2.20)
    (b) Motivação – Qual o nível de motivação para identificar e explorar a vulnerabilidade em questão? (Tabela 2.21)
    (c) Oportunidade – Que recursos e oportunidades são requeridas para encontrar e explorar a vulnerabilidade em questão? (Tabela 2.22)
    (d) Dimensão – Quantos elementos estão envolvidos no ataque? (Tabela 2.23)
2. Fatores inerentes à vulnerabilidade
    (a) Facilidade na identificação – Qual o grau de facilidade na descoberta da vulnerabilidade? (Tabela 2.24)
    (b) Facilidade na exploração – Qual o grau de facilidade na exploração da vulnerabilidade? (Tabela 2.25)
    (c) Conhecimento – O quão bem conhecida é esta vulnerabilidade para o grupo? (Tabela 2.26)
    (d) Deteção da intrusão – Qual é a probabilidade de a intrusão ser detetada? (Tabela 2.27)

Nome da opção	Classificação
Nenhum conhecimento técnico	1
Algum conhecimento técnico	3
Utilizador avançado em computadores	5
Redes e programação	6
Testes de Penetração	9

Tabela 2.20: OWASP: Fatores inerentes à ameaça - Nível de Perícia [31]

Nome da opção	Classificação
Pouca ou nenhuma recompensa	1
Alta recompensa	5
Possível recompensa	6

Tabela 2.21: OWASP: Fatores inerentes à ameaça - Motivação [31]

Nome da opção	Classificação
Acesso total ou requer recursos com custo elevado	0
Acesso especial ou recursos requeridos	4
Algum acesso ou recursos requeridos	7
Nenhum acesso ou recursos requeridos	9

Tabela 2.22: OWASP: Fatores inerentes à ameaça - Oportunidade [31]

Nome da opção	Classificação
Programadores	2
Administradores de sistema	2
Utilizadores internos	4
Parceiros	5
Utilizadores autenticados	6
Utilizadores anónimos vindos da Internet	9

Tabela 2.23: OWASP: Fatores inerentes à ameaça - Dimensão [31]

Nome da opção	Classificação
Particularmente impossível	1
Difícil	3
Fácil	7
Ferramentas automáticas disponíveis	9

Tabela 2.24: OWASP: Fatores inerentes à vulnerabilidade - Facilidade na identificação [31]

Nome da opção	Classificação
Teórico	1
Difícil	3
Fácil	7
Ferramentas automáticas disponíveis	9

Tabela 2.25: OWASP: Fatores inerentes à vulnerabilidade - Facilidade na exploração [31]

Nome da opção	Classificação
Desconhecida	1
Escondida	4
Obvia	6
Conhecida publicamente	9

Tabela 2.26: OWASP: Fatores inerentes à vulnerabilidade - Conhecimento [31]

Deteção ativa na aplicação	1
Registados e revistos	3
Registados sem revisão	6
Não registados	9

Tabela 2.27: OWASP: Fatores inerentes à vulnerabilidade - Deteção da Intrusão [31]

A *posteriori*, deve ser estimado o impacto causado pela exploração bem-sucedida. Deste modo, o terceiro passo é identificar e caraterizar os fatores que suportam o cálculo do segundo indicador da fórmula, o impacto. É considerado o impacto técnico que é caraterizado pelo impacto no sistema vulnerável e como tal é necessário estimar a perda na confidencialidade, na integridade, na disponibilidade e na responsabilidade. Para além do impacto técnico também é necessário estimar o impacto no negócio, que caracteriza a importância do ativo para o negócio da organização, e por este motivo devem ser estimados os prejuízos financeiros, os prejuízos na reputação, o não cumprimento e a violação na

privacidade. Assim sendo, é apresentado de seguida em maior detalhe as questões que têm de ser colocadas para determinar a opção mais indicada para cada fator/variável:

1. Fatores inerentes ao impacto técnico

   (a) Perda na confidencialidade - Quantos dados podem ser divulgados e o quão sensíveis são? (Tabela 2.28)

   (b) Perda na integridade – Quantidade de dados corrompidos e o quão danificados podem estar? (Tabela 2.29)

   (c) Perda na disponibilidade - Quanto serviço poderia ser perdido e quão vital é? (Tabela 2.30)

   (d) Perda na responsabilidade – Consegue-se descobrir os responsáveis pelo sucedido? (Tabela 2.31)

2. Fatores inerentes ao impacto no negócio

   (a) Prejuízo financeiro - Quanto prejuízo financeiro resultará de uma exploração? (Tabela 2.32)

   (b) Prejuízo na reputação – Pode uma exploração resultar em danos à reputação que possam prejudicar o negócio? (Tabela 2.33)

   (c) Não cumprimento - Quanta exposição o não cumprimento apresenta? (Tabela 2.34)

   (d) Violação na privacidade - Quanta informação pessoal pode ser divulgada? (Tabela 2.35)

Nome da opção	Classificação
Divulgado o mínimo de dados não sensíveis	2
Divulgado o mínimo de dados críticos	6
Divulgado muitos dados não sensíveis	6
Divulgado muitos dados críticos	7
Divulgado todo o tipo de informação	9

Tabela 2.28: OWASP: Fatores inerentes ao impacto técnico - Perda na Confidencialidade [31]

Nome da opção	Classificação
Poucos dados ligeiramente corrompidos	1
Poucos dados seriamente corrompidos	3
Muitos dados ligeiramente corrompidos	5
Muitos dados seriamente corrompidos	7
Todos os dados totalmente corrompidos	9

Tabela 2.29: OWASP: Fatores inerentes ao impacto técnico - Perda na Integridade [31]

Nome da opção	Classificação
Interrompido os mínimos serviços secundários	1
Interrompido os mínimos serviços primários	5
Interrompido muitos serviços secundários	5
Interrompido muitos serviços primários	7
Todos os serviços foram interrompidos	9

Tabela 2.30: OWASP: Fatores inerentes ao impacto técnico - Perda na Disponibilidade [31]

Nome da opção	Classificação
Totalmente rastreável	1
Possivelmente rastreável	7
Completamente anónimo	9

Tabela 2.31: OWASP: Fatores inerentes ao impacto técnico - Perda na responsabilidade [31]

Nome da opção	Classificação
Menos do que o custo para mitigar a vulnerabilidade	1
Efeito menor sobre o lucro anual	3
Efeito significativo sobre o lucro anual	7
Falência	9

Tabela 2.32: OWASP: Fatores inerentes ao impacto técnico - Prejuízo Financeiro [31]

Nome da opção	Classificação
Mínimo dano	1
Perda de grandes contas	4
Perda de *goodwill*	5
Danos à marca	9

Tabela 2.33: OWASP: Fatores inerentes ao impacto técnico - Prejuízo na Reputação [31]

Nome da opção	Classificação
Violação menor	2
Violação clara	5
Violação de alto perfil	7

Tabela 2.34: OWASP: Fatores inerentes ao impacto técnico - Não Cumprimento [31]

Nome da opção	Classificação
Um indivíduo	3
Centenas de pessoas	5
Milhares de pessoas	7
Milhões de pessoas	9

Tabela 2.35: OWASP: Fatores inerentes ao impacto técnico - Violação na Privacidade [31]

Após a atribuição dos valores referentes à verossimilhança e ao impacto, é necessário determinar a severidade do risco identificado no primeiro passo. Deste modo, no quarto passo é calculado o risco considerando as seguintes fórmulas:

Verosimilhanca = (Nivel de pericia + Motivacao + Oportunidade + Dimensao + Facilidade na identificacao + Facilidade de exploracao + Conhecimento + Detecao da intrusao)/8

Impacto tecnico = (Perda na confidencialidade + Perda na Integridade + Perda na Disponibilidade + Perda na Responsabilidade)/4

Impacto no negocio = (Prejuizo Financeiro + Prejuizo na reputação + Prejuizo no não cumprimento + Violacao na privacidade)/4

No caso da verosimilhança (*likelihood*), todos os fatores são estimados, enquanto no impacto, é necessário escolher entre o impacto técnico e o impacto no negócio. A decisão é tomada considerando a informação disponível pela organização, ou seja, se o ativo contiver uma criticidade associada com custos identificados, então deve ser escolhido o impacto no negócio mas se não existir nenhuma informação do ativo relativamente ao impacto no negócio, deve ser considerado o impacto técnico, ou seja, na perspetiva

do auditor de segurança quais são as potenciais perdas da exploração da vulnerabilidade identificada.

O resultado dos dois indicadores é quantitativo mas são correspondidos a *posteriori* em valores qualitativos (Figura 2.11). Como ilustrado na equação 2.5, o cálculo do risco equivale ao produto entre a verosimilhança (*likelihood*) e o impacto, contudo este produto não é realizado utilizando os valores quantitativos mas sim qualitativos e por este motivo foi definida pelos autores a matriz de risco apresentada na Figura 2.12.

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Figura 2.11: Níveis de Verosimilhança e Impacto [31]

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Figura 2.12: Severidade do risco [31]

Posteriormente, definido pelos autores como o quinto passo, decidem-se quais as vulnerabilidades a mitigar considerando as classificações encontradas e deste modo é realizada a priorização das mesmas atendendo aos níveis definidos (Figura 2.11). Como mencionado pelos autores, as vulnerabilidades com classificação mais elevada devem ser corrigidas primeiro.

Por último, o sexto passo destina-se à possibilidade de customizar este modelo de risco com o acréscimo de fatores importantes para a organização em específico. Os autores evidenciaram uma aplicação militar como exemplo, em que a perda humana ou a existência de informação classificada podem ser dados importantes a incluir no fator de impacto [31].

2.5 CWSS – Common Weakness Scoring System

O Common Weakness Scoring System (CWSS) é uma metodologia desenvolvida com o propósito de pontuar vulnerabilidades e consequentemente facilitar a priorização das

mesmas [15]. Esta metodologia foi desenvolvida pelo MITRE, uma organização Americana sem fins lucrativos que gere centros de pesquisa e desenvolvimento financiados pelo governo federal (FFRDCs) que alicerçam várias agências governamentais dos Estados Unidos da América (EUA) [20]. O CWSS faz parte do projeto *Common Weakness Enumeration* [21] patrocinado pelo programa *Software Assurance* no posto de Segurança Cibernética e Comunicação do Departamento de Segurança Interna dos EUA [15].

O modelo empregue é quantitativo e à semelhança do CVSS, esta metodologia está divida em três grupos de métricas: Base (*Base Finding*), Superfície de Ataque e Ambiental [15].

A métrica base é constituída pelo risco inerente à vulnerabilidade, pela credibilidade na fonte que publicou a vulnerabilidade e pelos controlos de segurança existentes. Deste modo, é composta por cinco fatores: o impacto técnico, privilégios adquiridos, camada de privilégios adquiridos, eficiência dos controlos internos e grau de confiança. O impacto técnico representa o resultado produzido pela exploração bem-sucedida da vulnerabilidade, assumindo que o atacante consegue alcançá-la e consequentemente explorá-la. Os privilégios adquiridos, como o nome indica, são os privilégios obtidos pelo atacante na exploração da vulnerabilidade. A camada de privilégios adquiridos é a camada operacional que o atacante conseguiu ultrapassar para escalar privilégios. A eficiência dos controlos denota a capacidade de deteção e prevenção, impedindo que o ataque seja bem-sucedido. Por último, o grau de confiança determina o nível de credibilidade na fonte que reportou o problema e a confirmação que este problema é uma vulnerabilidade possível de ser utilizada por um atacante. Os *scores* da métrica base podem variar entre 0 e 100.

A métrica superfície de ataque é constituída pelos controlos que o atacante terá de ultrapassar para explorar com sucesso a vulnerabilidade. Desta forma, é composta por seis fatores: privilégios requeridos, camada de privilégios requeridos, vetor de ataque, robustez na autenticação, nível de interação e âmbito. Os privilégios requeridos são caraterizados pelo tipo de privilégios que um atacante já deve possuir para alcançar o componente vulnerável. A camada de privilégios requeridos destina-se à camada operacional a que o atacante deve ter privilégios para conseguir explorar a vulnerabilidade. O vetor de ataque indica a comunicação de rede necessária para alcançar o componente vulnerável. A robustez na autenticação quantifica o nível de dificuldade necessário para aceder ao componente vulnerável. O nível de interação reflete a necessidade de interação do utilizador para o ataque ser bem-sucedido. O âmbito designa a presença da vulnerabilidade em todas as versões do *software* ou se apenas está presente num conjunto limitado de plataformas e/ou configurações. Os *scores* da métrica superfície de ataque apenas variam entre 0 e 1.

A métrica ambiental é constituída pelas caraterísticas da vulnerabilidade que são específicas para cada entidade. Como tal, é composta por cinco fatores: impacto no negócio, probabilidade de identificação, probabilidade de exploração, eficiência dos controlos ex-

ternos e prevalência. O impacto no negócio determina o potencial impacto financeiro e reputacional para a entidade. A probabilidade de identificação e a probabilidade de exploração estimam exequibilidade de identificar e explorar a vulnerabilidade em questão. A eficiência dos controlos externos denota a capacidade externa de deteção e prevenção, impedindo que o ataque seja bem-sucedido. Por fim, a prevalência identifica a frequência com que este tipo de vulnerabilidade surge no *software*. Os *scores* da métrica ambiental à semelhança da métrica superfície de ataque apenas variam entre 0 e 1.

Esta metodologia oferece a possibilidade de atribuir *scores* customizados para a maioria dos fatores [15].

As fórmulas definidas para o cálculo da severidade da vulnerabilidade são apresentadas de seguida:

Score = MetricaBase * MetricaSuperficieDeAtaque * MetricaAmbiental

MetricaBase = [(10 * ImpactoTecnico + 5*(PrivilegiosAdquiridos + CamadaPrivilegiosAdquiridos) + 5*GrauDeConfianca) * f(ImpactoTecnico) * EficienciaDosControlosInternos] * 4.0

f(ImpactoTécnico) = 0 se ImpactoTécnico = 0; caso contrário f(ImpactoTécnico) = 1.

À semelhança do CVSS, o impacto técnico é utilizado para garantir que se não existir impacto na exploração de uma vulnerabilidade, não resulte num valor diferente de 0, considerando que os outros fatores também contam para o *score*.

MetricaSuperficieDeAtaque = [20*(PrivilegiosRequeridos + CamadaDePrivilegiosRequeridos + VetorDeAtaque) + 20*Foco + 15*NivelDeInteracao + 5*RobustezNaAutenticacao] / 100.0

MetricaAmbiental = [(10*ImpactoNoNegocio + 3*ProbabilidadeDeIdentificacao + 4*ProbabilidadeDeExploracao + 3*Prevalencia) * f(ImpactoNoNegocio) * EficienciaDosControlosExternos] / 20.0

f(ImpactoNoNegocio) = 0 se ImpactoNoNegocio == 0; caso contrário f(ImpactoNoNegocio) = 1

2.6 Análise das metodologias apresentadas

Como descrito no presente capítulo, foram desenvolvidas várias metodologias com o propósito de auxiliar as organizações a priorizar as vulnerabilidades identificadas nos seus

ativos, tarefa esta árdua de atingir devido às centenas de vulnerabilidades com classificações elevadas [14, 39].

O CVSS é a metodologia mais conhecida e utilizada por várias entidades na atribuição de pesos às vulnerabilidades detetadas nos seus sistemas e ativos [46]. Devido aos vários problemas identificados no CVSS versão 2, foram desenvolvidas e melhoradas duas metodologias já descritas nas secções 2.2 e 2.3. No entanto, foram considerados pressupostos no WIVSS que não se aplicam a todo o público alvo, dado que foi considerado o impacto na confidencialidade o mais crítico, seguido do impacto na integridade e por último o impacto na disponibilidade. Contudo, se a empresa apenas disponibilizar um serviço de notícias públicas na Internet, terá muito mais impacto a alteração ou indisponibilização deste serviço, ou seja, a integridade e disponibilidade terão muito mais peso para esta organização do que a confidencialidade, tudo depende do tipo de negócio. O VRSS, por outro lado, é baseado nos tipos de vulnerabilidades mais conhecidos e disponibilizados pelo CWE [21]. Esta abordagem limita a atribuição de pesos a todas as vulnerabilidades dado que existem cada vez mais tipos de vulnerabilidades. O número de tipos de vulnerabilidades não deve ser considerado um valor estático e como exemplo do exposto temos o *Cross-site flashing* que à semelhança do *Cross-site scripting* é necessário injetar código neste caso em flash, que como é possível verificar na tabela 2.19 não foi considerado.

A ORACLE adicionou mais um valor à métrica de impacto da versão 2 do CVSS denominada por Parcial+. A opção Parcial+ engloba vários recursos que foram afetados pela exploração bem sucedida da vulnerabilidade, como por exemplo, todas as tabelas da base de dados, comprometer toda a aplicação ou sistema [27]. A opção Parcial engloba apenas um número limitado de recursos impactados, como por exemplo, uma tabela específica da base de dados. Posteriormente foi proposta uma melhoria ao CVSS versão 2, em que foi sugerido a inserção de um quarto valor à sub-métrica de impacto, que podia ser igual ao Parcial+ (*"Partial+"*) da Oracle [6]. A definição dos valores "nenhum" (*None*) e total (*Complete*) mantinham-se mas o "parcial" (*Partial*) seria alterado para criar mais granularidade entre este e o novo valor "Parcial+" (*Partial+*). As definições destes dois valores encontram-se de seguida:

Impacto na confidencialidade

1. "Parcial" (*Partial*) - Um sub-conjunto de dados acessíveis na aplicação podem ser divulgados.

2. "Parcial+" (*Partial+*) - Todos os dados acessíveis na aplicação podem ser divulgados.

Impacto na integridade

1. "Parcial" (*Partial*) - Um sub-conjunto de dados acessíveis na aplicação podem ser manipulados.

2. ”Parcial+” (*Partial+*) - Todos os dados acessíveis na aplicação podem ser manipulados.

Impacto na disponibilidade

1. ”Parcial” (*Partial*) - Um sub-conjunto de funcionalidades da aplicação não está disponível ou a aplicação está disponível por um curto período de tempo.

2. ”Parcial+” (*Partial+*) - Toda a aplicação está indisponível até, por exemplo, um *restart/reboot*.

O valor definido para esta nova opção não foi publicamente disponibilizado pela ORACLE, no entanto com versão 3 do CVSS esta opção não foi incluída e a proposta de melhoria também não foi aceite.

Na versão 3 do CVSS, identificaram-se várias melhorias comparativamente à versão 2 [34], no entanto foram identificados vários problemas [35, 36, 37, 38, 39], um dos quais causa bastante impacto no objetivo principal do desenvolvimento desta metodologia, pois se na versão 2 já existiam várias vulnerabilidades com pesos elevados na versão 3 observou-se um aumento significativo na severidade das vulnerabilidades, existindo um grande número de vulnerabilidades nos níveis alto e crítico e consequentemente uma redução no número de vulnerabilidades nos níveis médio e baixo [33]. Como o objetivo principal deste tipo de metodologias é apoiar as organizações na priorização de vulnerabilidades, com o problema anteriormente indicado as organizações dificilmente conseguem priorizar as vulnerabilidades de modo a identificar as que são realmente críticas e que necessitam de ser prontamente tratadas - ”When every defect is high priority... Nothing is!”[39].

Em conclusão, a versão 3 do CVSS tem sem dúvida vários problemas relativamente à diversidade de valores e quantidade de vulnerabilidades nas classificações críticas e altas, como já apontado por várias comunidades e elementos/equipas de segurança de enumeras organizações [33]. Também já foram enviadas várias propostas de melhoria para colmatar alguns dos problemas identificados [12]. Algumas destas melhorias já foram aprovadas, no entanto nenhuma das apresentadas consideram os dois problemas que se pretende endereçar na presente dissertação.

Com o mesmo propósito dos autores do WIVSS e VRSS que tentaram melhorar o CVSS versão 2 para auxiliar as milhares ou até mesmo milhões de organizações com problemas na priorização de vulnerabilidades, esta dissertação tem como propósito melhorar a metodologia mais reputada e empregue nas organizações com o contributo de diversificar a severidade das vulnerabilidades identificadas e diminuir a quantidade de vulnerabilidades nos valores críticos e altos. Deste modo, possibilita que a priorização de vulnerabilidades se torne uma tarefa mais fácil, útil e eficiente.

Capítulo 3

Apresentação de uma proposta de melhoria ao CVSS

Nos dias que decorrem, cada vez mais é importante gerir as dezenas, centenas ou milhares de vulnerabilidades identificadas pelas equipas de auditoria de segurança nos sistemas, ativos e/ou aplicações com o propósito de mitigar posteriormente as vulnerabilidades mais críticas para o negócio da organização. É, desta forma, necessário implementar ou optar por uma metodologia que auxilie no processo de priorização de vulnerabilidades.

O CVSS é sem dúvida o sistema de avaliação de vulnerabilidades mais adotado por várias organizações, no entanto tem diversos problemas, já mencionados no capítulo 2, que dificultam a priorização das vulnerabilidades. Como tal, o objetivo deste trabalho é propor uma extensão ao CVSS que pretende aumentar a diversidade de valores e diminuir a quantidade de classificações críticas e altas.

3.1 Análise do sistema de avaliação de vulnerabilidades - CVSS

Nas subsecções seguintes vão ser evidenciados os dois problemas do CVSS que se pretende endereçar.

3.1.1 Quantidade de vulnerabilidades nas classificações críticas e altas

Em 2016 foram identificadas 6447 vulnerabilidades e em 2017 mais do dobro, 14650 [25], como tal é necessário gerir a grande quantidade de vulnerabilidades, de modo a mitigá-las pela severidade. No entanto, se já existia uma grande quantidade de vulnerabilidades na classificação alta da versão 2 do CVSS, na versão 3 verifica-se um aumento significativo nas vulnerabilidades com severidade mais elevada, com 4314 e 8728 respetivamente (Figura 3.1). Estas estatísticas mostram que várias vulnerabilidades na versão 2 pertencentes às classificações baixa e média, pertencem agora às classificações alta e crítica [39].

A diferença notória entre a versão 2 e a versão 3 provém do fator âmbito (”*scope*”) adicionado na versão 3, visto que basta o âmbito alterar para a severidade das vulnerabilidades aumentar significativamente. Para além disso, caso o âmbito altere, o impacto na confidencialidade, integridade e disponibilidade deve refletir o maior impacto entre o componente vulnerável e componente impactado [37]. Analisando os exemplos ilustrados pelo FIRST [11] da maneira como a severidade das vulnerabilidades eram avaliadas com a versão 2 e agora são classificadas na versão 3, observa-se que este aumento nas classificações alta e crítica deve-se ao indicado anteriormente. Como por exemplo, a vulnerabilidade CVE-2013-6014 é classificada na versão 2 com 6.1 e na versão 3 com 9.3. Analisando as diferenças apresentadas de seguida, verifica-se que o âmbito altera e desta forma, o impacto é refletido considerando o pior caso, que neste caso é o componente impactado:

Vetor CVSSv2.0: AV:A/AC:L/Au:N/**C:N/I:C/A:N**
Vetor CVSSv3.0: AV:A/AC:L/PR:N/UI:N/**S:C/C:H/I:N/A:H**

Desta forma, o impacto na integridade com valor total atribuído na versão 2 é alterado para o valor nenhum na versão 3, visto que o impacto sobre o componente impactado é maior que o impacto sobre o componente vulnerável.

Devido a esta discrepância de valores e considerando que existem várias vulnerabilidades com severidade crítica e alta, constata-se a dificuldade, já indicada anteriormente, em priorizar vulnerabilidades. Deste modo, é necessário diminuir o número de vulnerabilidades nas classificações elevadas.

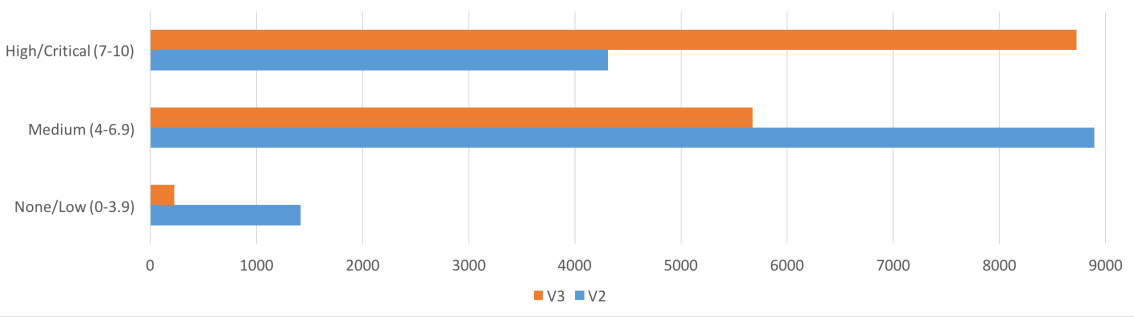

Figura 3.1: Número de vulnerabilidades por níveis de classificação - comparação entre versão 2 e versão 3 do CVSS

3.1.2 Diversidade de valores

Considerando os valores disponibilizados para a avaliação de vulnerabilidades, é necessário perceber a quantidade de colisões[1] em cada classificação no intervalo de [0,10]

[1]Uma colisão é a obtenção de dois ou mais valores iguais na escala de [0,10], em que duas ou mais vulnerabilidades obtenham a mesma severidade mas que os valores escolhidos para cada uma são diferentes,

em que o espaçamento é de 0.1 em 0.1 (p.e. 0, 0.1, 0.2, 0.3, 0.4, ... , 9.9, 10), o que corresponde a 101 valores.

Este estudo considera tanto a métrica base, sendo esta obrigatória para a avaliação de vulnerabilidades, como a métrica ambiental que considera os requisitos na confidencialidade, integridade e disponibilidade do ativo na entidade. Estes requisitos são importantes para o estudo das vulnerabilidades da EDP.

Algorithm 1: Algoritmo que obtém o número de colisões por *score* resultante do cálculo dos *scores* de todas as combinações possíveis na métrica base

```
while contador > len(combinacoes_possiveis) do
    Calcular isc_base;
    if ambito == nao_altera then
        isc = 6.42 * isc_base;
    else
        isc = 7.52 * (isc_base - 0.029) - 3.25 * pow(isc_base - 0.02, 15);
    if privilegios_requeridos == 0.62 AND ambito == altera then
        privilegios_requeridos = 0.68;
    if privilegios_requeridos == 0.27 AND ambito == altera then
        privilegios_requeridos = 0.50;
    exploracao = 8.22 * superficie_ataque * complexidade_ataque *
     privilegios_requeridos * interacao_utilizador;
    if isc <= 0 then
        base_score = 0;
    else
        if ambito == nao_altera then
            base_score = _round_up_1(min(isc + exploracao, 10));
        else
            base_score = _round_up_1(min(1.08 * (isc + exploracao), 10));
    Guarda no resultado cada base_score;
    contador+=1;
Conta as colisões no resultado e guarda no counter;
while j <= 10 do
    Guarda o j com counter[j] no resultado_ordenado;
    j+=0.1;
Imprime resultado_ordenado;
```

Desta forma, foi desenvolvido um algoritmo (Algoritmo 1) para calcular todas as combinações possíveis[2] com o objetivo de obter a quantidade de colisões para cada seve-

p.e. as seguintes combinações de fatores da métrica base obtêm a mesma avaliação:
AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Em resumo, as colisões dão indicação de probabilidade de ocorrência de determinada classificação.

[2]As combinações são calculadas tendo em consideração o número de valores numéricos existentes em

ridade na escala já indicada anteriormente. As fórmulas existentes no algoritmo podem ser revisitadas no capítulo 2 na secção 2.1.

Com o apoio deste algoritmo, identificou-se que apenas se obtém 84 classificações diferentes de 101 possíveis, independentemente dos valores escolhidos para cada fator, o que mostra limitações na métrica. Como é possível verificar na figura 3.2, os valores em falta são maioritariamente referentes ao nível qualitativo baixo, o que significa que vulnerabilidades que à partida deveriam ser pontuadas com uma pontuação mínima, neste caso podem ser pontuadas acima de 1.5. Consequentemente, a falta dos valores em questão, pode influenciar os resultados finais de todas as vulnerabilidades com *scores* superiores, atribuindo mais importância às vulnerabilidades menos importantes. Para além dos 15 valores ([0.1,1.6[) em falta, existem mais dois referentes à escala qualitativa crítica, que também podem ajudar na diminuição de colisões nas vulnerabilidades mais críticas, sendo estes, o 9.5 e o 9.7.

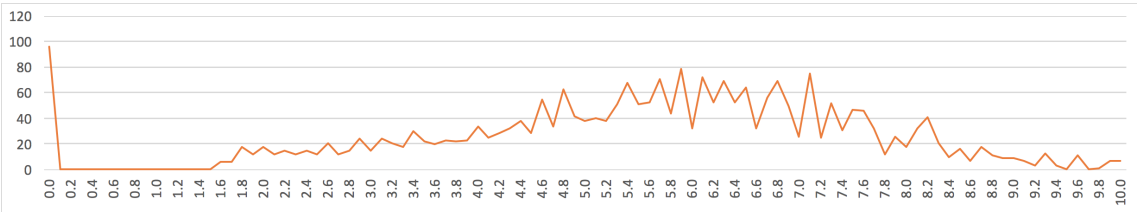

Figura 3.2: Distribuição de valores - Métrica base com os 3 valores por defeito

O mesmo estudo foi efetuado para a métrica ambiental. Com a utilização do algoritmo anterior, foram introduzidos os fatores referentes aos requisitos na confidencialidade, integridade e disponibilidade como também os respetivos valores numéricos, para serem considerados nas combinações. Dado que para o estudo em causa não é necessário alterar os valores da métrica base, os restantes fatores da métrica ambiental não foram considerados. Também foram adicionadas as fórmulas referentes à métrica ambiental para, desta forma, avaliar cada combinação e obter as colisões da métrica ambiental na escala [0,10] (Algoritmo 2).

A distribuição de valores é bastante mais favorável, uma vez que se obteve 93 valores em 101 possíveis (Figura 3.3). No entanto, verifica-se novamente a existência da mesma limitação que a métrica base, com a diferença que é em menos quantidade e apenas referente ao nível qualitativo baixo.

O número total de combinações consideradas no gráfico da Figura 3.2 é 2592, enquanto que no da Figura 3.3 esse valor é 165888.

cada fator. Desta forma, contando o número de valores existentes para cada fator e fazendo o produto do número total de cada fator, obtém-se o número de combinações possíveis. Cada combinação é dada como *input* para o cálculo da métrica base.

Algorithm 2: Algoritmo que obtém o número de colisões por *score* resultante do cálculo dos *scores* de todas as combinações possíveis na métrica ambiental

```
while contador > len(combinacoes_possiveis) do
    Calcular isc_base;
    if ambito == nao_altera then
        isc = 6.42 * isc_base;
    else
        isc = 7.52 * (isc_base - 0.029) - 3.25 * pow(isc_base - 0.02, 15);
    if privilegios_requeridos == 0.62 AND ambito == altera then
        privilegios_requeridos = 0.68;
    if privilegios_requeridos == 0.27 AND ambito == altera then
        privilegios_requeridos = 0.50;
    exploracao = 8.22 * superficie_ataque * complexidade_ataque *
     privilegios_requeridos * interacao_utilizador;
    if isc <= 0 then
        base_score = 0;
    else
        if ambito == nao_altera then
            base_score = _round_up_1(min(isc + exploracao, 10));
        else
            base_score = _round_up_1(min(1.08 * (isc + exploracao), 10));
    isc_alterado = min((1 - (1 - conf_impact * conf_req) * (1 -integ_impact *
     integ_req) * (1 - avail_impact * avail_req)), 0.915);
    exploracao_alterada = exploracao;
    ambito_alterado = ambito;
    if ambito_alterado == nao_altera OR ambito_alterado is None AND ambito
     == nao_altera then
        misc = 6.42 * isc_alterado;
        ambiental_score = _round_up_1(_round_up_1(min((misc +
         exploracao_alterada), 10)) * exploit * remediation_level *
         report_confidence);
    else
        misc = (7.52 * (isc_alterado - 0.029)) - (3.25 * (pow((isc_alterado -
         0.02), 15)));
        ambiental_score = _round_up_1(_round_up_1(min(1.08 * (misc +
         exploracao_alterada), 10)) * exploit * remediation_level *
         report_confidence);
    if misc <= 0 then
        ambiental_score = 0;
    Guarda no resultado cada ambiental_score;
    contador+=1;
Conta as colisões no resultado e guarda no counter;
while j <= 10 do
    Guarda o j com counter[j] no resultado_ordenado;
    j+=0.1;
Imprime resultado_ordenado;
```

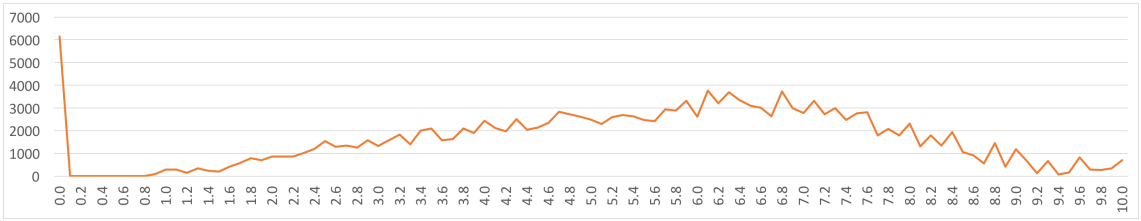

Figura 3.3: Distribuição de valores - Métrica base e ambiental com os 3 valores por defeito

3.2 Definição de critérios

Como analisado anteriormente, o CVSS versão 3 tem limitações na escala definida, dado que nenhuma das combinações possíveis obtém os seguintes valores na métrica base: [0.1,1.6[, 9.5 e 9.7. O mesmo acontece na métrica ambiental mas em menos quantidade. Como tal, um dos critérios para a extensão de melhoria do CVSS é o seguinte:

- Obter o máximo de valores possíveis na escala de [0,10], igual ou aproximado a 101 valores.

Através da figura 3.1 identifica-se uma grande quantidade de vulnerabilidades nas classificações alta e crítica, o que dificulta a priorização de vulnerabilidades. Deste modo, o segundo critério a considerar é o seguinte:

- A distribuição de valores na classificação alta e crítica deve tender para uma distribuição mais homogénea e em menos quantidade.

Tendo os critérios definidos, é necessário perceber de que forma podemos atingir estes dois objetivos. Com certeza que devem existir vários caminhos para obter os resultados desejados, como alterar as formulas do CVSS, alterar os valores numéricos referentes aos factores, entre outras. Todavia, analisando em mais detalhe a quantidade de opções disponíveis para cada fator, surge a necessidade de ter mais opções na sub-métrica de impacto da métrica base, que são disponibilizados apenas três valores para a sub-métrica de impacto, sendo estes, nenhum, baixo e alto. Estas opções são limitadas e, como tal, a abordagem que se optou foi aumentar a granularidade de valores nos fatores de impacto. Por este motivo, nas seguintes secções vão ser apresentados dois novos valores para a sub-métrica de impacto, denominados por médio e muito-baixo.

3.3 Proposta de um novo valor

A sub-métrica de impacto consiste em três tipos de impacto, o impacto na confidencialidade, integridade e disponibilidade. Cada um destes impactos contêm o valor nenhum, baixo e alto. Considerando que o valor baixo tem o valor numérico 0.22 e a opção alto

tem o valor numérico 0.56, significa que no total é possível escolher entre 33 valores diferentes para o novo valor médio.

Na próxima sub-secção, vai ser exposto o método de escolha do valor numérico correspondente ao valor médio.

3.3.1 Métrica Base - Análise das métricas em concordância com os critérios definidos

Com base no algoritmo 1 foi introduzido um novo valor que pode variar entre a escala [0.23,0.56[, uma vez que o valor numérico baixo é 0.22 e o valor numérico alto é 0.56. Neste sentido, para cada valor pertencente ao intervalo indicado foram contabilizadas as colisões para a métrica base. É possível observar na tabela 3.1 que conseguimos aumentar a distribuição de valores visto que obtemos mais dois valores na escala [0,10], que totaliza uma classificação de 86 valores em vez de 84.

Uma vez que para atingir o primeiro critério é necessário obter uma maior distribuição de valores e tendo em consideração a tabela 3.1, os valores a considerar são: [0.31, 0.33], 0.36, [0.38, 0.40] e [0.43,0.55].

Contudo também é necessário garantir a diminuição de valores nas classificações alta e crítica. Neste sentido, foi calculada a percentagem de valores nas classificações nenhuma, baixa, média, alta e crítica, como também a curtose[3] total, curtose nos valores altos e curtose nos valores críticos (Tabela 3.2) que auxiliam a definição deste novo valor considerando o segundo critério. Tendo em vista os valores que estão de acordo com o primeiro critério, é possível observar na tabela 3.2 que os valores com menor percentagem nas classificações elevadas comparativamente aos valores por omissão da métrica base são o 0.31, 0.32 e 0.33. Relativamente à curtose, tanto na classificação alta como crítica, o valor mais favorável é o 0.32, o que significa que escolhendo o mesmo para o valor médio, a distribuição nas classificações elevadas vai ser mais homogénea tanto nos valores elevados como no total.

Pela figura 3.4 é possível observar que em comparação com os valores por defeito existe uma distribuição mais homogénea nos valores altos e críticos porém mais significativa nos valores altos. Dado que é possível obter mais dois valores do que os valores por defeito, o 9.5 e 9.7, representados na figura 3.4 com 3 e 6 colisões respetivamente, é expetável que estes valores auxiliem a redução das colisões nos valores críticos.

Se apenas fossem considerados os resultados da métrica base, o valor escolhido seria o 0.32, no entanto é necessário verificar se este valor continua a ser o mais favorável na métrica ambiental. Como tal, é apresentado de seguida o mesmo estudo para as classificações da métrica ambiental.

[3]Mede o achatamento da curva, ou seja, quanto mais pequena e abaixo de zero for, mais linear é a distribuição de probabilidade

Valor Médio	Total de *Scores* - Métrica Base	Total de *Scores* - Métrica Ambiental
0.23	84	93
0.24	84	93
0.25	84	93
0.26	85	93
0.27	85	93
0.28	85	93
0.29	85	93
0.30	85	93
0.31	86	93
0.32	86	93
0.33	86	93
0.34	85	93
0.35	85	93
0.36	86	93
0.37	85	93
0.38	86	93
0.39	86	93
0.40	86	93
0.41	85	93
0.42	85	93
0.43	86	93
0.44	86	93
0.45	86	93
0.46	86	93
0.47	86	93
0.48	86	93
0.49	86	93
0.50	86	93
0.51	86	93
0.52	86	93
0.53	86	93
0.54	86	93
0.55	86	93

Tabela 3.1: Contabilização de *Scores* da métrica base e ambiental com quatro valores na sub-métrica impacto

Métrica Base	Valor Médio	%Nenhum [0]	%Baixo [0.1,4)	%Médio [4,7)	%Alto [7,9)	%Critico [9,10]	Curtose Alta	Curtose Crítica	Curtose Total
	0.23	1.6	18.3	59.6	18.6	1.8	-0,24	-1,15	-1,26
	0.24	1.6	17.8	59.8	19.0	1.8	-0,93	-1,39	-1,22
	0.25	1.6	17.4	60.1	19.1	1.9	-1,04	-1,01	-1,25
	0.26	1.6	16.5	60.5	19.5	1.9	-0,50	-0,84	-1,03
	0.27	1.6	15.7	61.0	19.8	1.9	0,02	-1,39	-1,13
	0.28	1.6	15.1	61.0	20.2	2.1	1,36	-1,20	-0,81
	0.29	1.6	14.3	61.3	20.7	2.1	-0,07	-1,13	-0,88
	0.30	1.6	13.9	61.3	20.9	2.3	-1,17	0,80	-1,09
	0.31	1.6	13.7	61.1	21.4	2.3	-0,93	1,67	-1,01
	0.32	1.6	12.7	61.5	22.0	2.3	-0,79	-1,95	-1,09
	0.33	1.6	12.3	61.7	22.1	2.3	1,34	-1,86	-0,85
	0.34	1.6	11.8	61.5	22.8	2.3	2,48	-1,68	-0,86
	0.35	1.6	11.7	61.3	23.0	2.4	-0,02	-0,65	-0,90
	0.36	1.6	11.2	61.7	23.1	2.5	0,22	0,69	-1,05
	0.37	1.6	10.8	61.2	23.8	2.6	-0,86	0,99	-0,90
	0.38	1.6	10.8	60.9	24.1	2.7	-1,27	-0,58	-0,96
4 valores	0.39	1.6	10.4	60.6	24.8	2.7	-1.18	-1.38	-0.82
	0.40	1.6	9.90	60.6	25.2	2.7	-1.41	-1.05	-0.87
	0.41	1.6	9.80	60.3	25.6	2.8	-0.25	-1.49	-0.89
	0.42	1.6	9.70	59.7	26.1	2.9	-0.74	-1.64	-0.93
	0.43	1.6	9.10	60.0	26.3	3.0	-1.08	-1.75	-0.59
	0.44	1.6	8.80	59.4	27.0	3.3	-0.78	-1.16	-0.72
	0.45	1.6	8.60	58.8	27.8	3.3	-0.88	0.47	-1.03
	0.46	1.6	8.30	58.4	28.4	3.3	-0.84	0.39	-0.96
	0.47	1.6	8.00	58.4	28.5	3.5	-0.89	-0.73	-0.91
	0.48	1.6	7.80	58.2	28.9	3.5	0.05	-0.23	-0.83
	0.49	1.6	7.70	57.3	29.9	3.5	-1.37	-0.08	-0.78
	0.50	1.6	7.60	57.1	30.0	3.6	-1.14	-1.10	-1.01
	0.51	1.6	7.50	56.6	30.5	3.8	-1.52	-1.48	-0.91
	0.52	1.6	7.50	56.4	30.7	3.8	-1.39	-0.96	-0.84
	0.53	1.6	7.30	55.5	31.7	3.9	-1.47	-1.15	-0.85
	0.54	1.6	7.20	55.3	32.0	3.9	-0.37	-0.63	-0.78
	0.55	1.6	7.10	54.8	32.5	4.1	-0.21	-0.86	-0.19
3 valores	-	3.7	16.0	56.5	21.4	2.4	1,33	1,13	0,09

Tabela 3.2: Métricas para a escolha do quarto valor comparativamente ao valores por defeito - Métrica Base - percentagem de valores nas classificações qualitativas e curtose

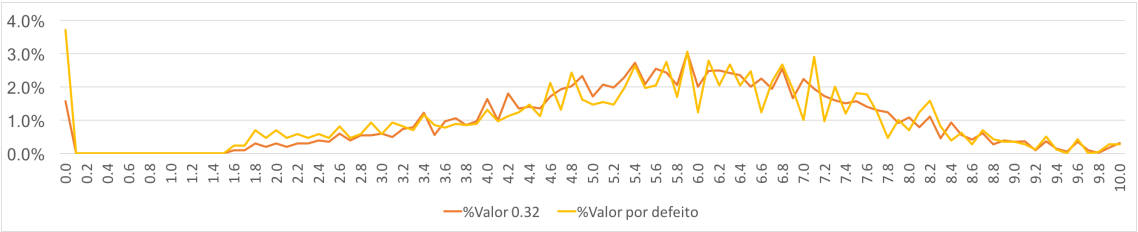

Figura 3.4: Distribuição de valores em proporção - Métrica base com os 3 valores por defeito e a adição do valor 0.32

3.3.2 Métrica Ambiental - Análise das métricas em concordância com os critérios definidos

Neste caso, em todos os valores numéricos a distribuição de classificações é idêntica, com 93 valores diferentes (Tabela 3.1). Como tal, o primeiro critério é cumprido com qualquer um destes valores.

Em relação ao segundo critério e tendo como base as mesmas métricas (Tabela 3.3), os valores numéricos mais favoráveis são os valores referentes ao intervalo [0.23,0.32], dado que a percentagem de valores nas classificações elevadas é menor que os restantes valores, mesmo comparando estes com os valores por omissão. No que diz respeito aos valores da curtose, o valor numérico 0.32 destaca-se nas classificações alta e crítica, dado

que se obtém valores menores que os restantes. Desta forma, a distribuição vai ser mais homogénea nos valores elevados e considerando que a percentagem nas classificações elevadas é menor comparativamente aos valores por omissão consegue-se, desta forma, diminuir o número de colisões nas classificações alta e crítica.

Métrica Base	Valor Médio	%Nenhum [0]	%Baixo [0.1,4)	%Médio [4,7)	%Alto [7,9)	%Critico [9,10]	Curtose Alta	Curtose Crítica	Curtose Total
	0.23	1.6	21.4	54.4	20.1	2.6	-1,11	0,00	-1,54
	0.24	1.6	20.8	54.7	20.3	2.6	-1,13	0,83	-1,52
	0.25	1.6	20.2	54.9	20.7	2.6	-1,07	1,23	-1,53
	0.26	1.6	19.5	55.3	21.0	2.7	-1,05	1,05	-1,51
	0.27	1.6	18.8	55.6	21.3	2.7	-1,18	-0,32	-1,50
	0.28	1.6	18.3	55.8	21.6	2.7	-0,97	-0,20	-1,46
	0.29	1.6	17.7	56.1	21.9	2.8	-0,91	-0,41	-1,44
	0.30	1.6	17.2	56.1	22.4	2.8	-0,98	0,86	-1,46
	0.31	1.6	16.8	56 .0	22.7	2.9	-1,09	0,78	-1,47
	0.32	1.6	16.2	56.2	23.2	2.9	-1,16	-0,45	-1,42
	0.33	1.6	15.8	56.2	23.5	3.0	-1,10	-0,29	-1,40
	0.34	1.6	15.4	56.1	23.9	3.0	-1,13	0,91	-1,42
	0.35	1.6	15.0	55.9	24.4	3.1	-1,13	1,58	-1,34
	0.36	1.6	14.6	56 .0	24.7	3.2	-1,16	1,02	-1,32
	0.37	1.6	14.3	55.7	25.2	3.2	-1,09	1,14	-1,32
	0.38	1.6	14.1	55.4	25.6	3.3	-0,95	1,02	-1,30
4 valores	0.39	1.6	13.8	55.2	26.1	3.4	-1,05	0,43	-1,29
	0.40	1.6	13.4	55 .0	26.6	3.4	-1,01	0,71	-1,27
	0.41	1.6	13.2	54.7	27.1	3.5	-1,23	-0,85	-1,20
	0.42	1.6	12.9	54.4	27.5	3.6	-1,23	-0,16	-1,25
	0.43	1.6	12.6	54.3	27.8	3.7	-1,15	0,24	-1,16
	0.44	1.6	12.4	53.8	28.3	3.8	-0,85	0,53	-1,12
	0.45	1.6	12.2	53.5	28.8	3.9	-0,86	1,14	-1,17
	0.46	1.6	12.0	53.0	29.4	4.0	-0,82	2,31	-1,13
	0.47	1.6	11.8	52.8	29.8	4.0	-1,05	0,40	-1,07
	0.48	1.6	11.6	52.5	30.2	4.1	-1,02	0,33	-1,07
	0.49	1.6	11.6	52.0	30.7	4.2	-1,15	0,00	-1,00
	0.50	1.6	11.5	51.6	31.0	4.3	-0,89	0,14	-1,01
	0.51	1.6	11.3	51.2	31.5	4.4	-0,75	2,11	-0,99
	0.52	1.6	11.2	50.8	31.9	4.5	-1,05	0,72	-0,94
	0.53	1.6	11.0	50.5	32.4	4.6	-1,07	1,52	-0,84
	0.54	1.6	10.9	50.1	32.8	4.7	-1,00	1,44	-0,73
	0.55	1.6	10.8	49.8	33.1	4.8	-1,02	1,23	-0,75
3 valores	-	3.7	20.1	49.7	23.3	3.2	-0,91	-0,26	0,57

Tabela 3.3: Métricas para a escolha do quarto valor comparativamente aos valores por defeito - Métrica Ambiental - percentagem de valores nas classificações qualitativas e Curtose

Tendo em conta o estudo anteriormente apresentado, o valor numérico proposto para o valor médio é o 0.32. Na tabela 3.4 é adicionado aos fatores de impacto na confidencialidade, integridade e disponibilidade o novo valor médio e o valor numérico respetivo.

Opção	Valor
Alto	0.56
Médio	0.32
Baixo	0.22
Nenhum	0

Tabela 3.4: Métrica Base - Impacto na Confidencialidade, Integridade e disponibilidade

À semelhança da métrica base é possível observar na figura 3.5 que em comparação com os valores por omissão existe uma distribuição mais homogénea nos valores altos e críticos, no entanto é mais significativo nos valores da classificação alta.

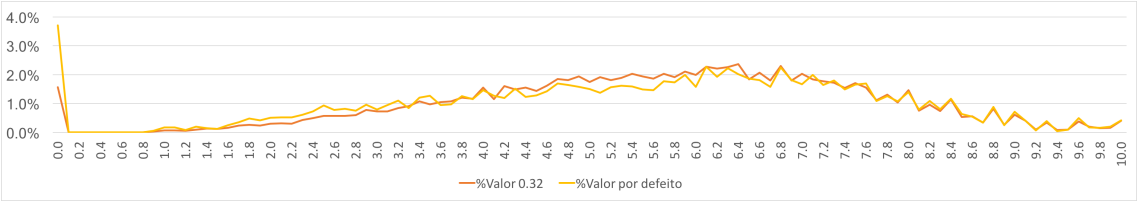

Figura 3.5: Distribuição de valores em proporção - Métrica Ambiental com os 3 valores por defeito e o novo valor 0.32

Contudo, ainda não foi cumprido na totalidade o primeiro critério dado que não aumenta consideravelmente a distribuição de classificações. Como tal, tomou-se a decisão de propor mais um valor na sub-métrica de impacto, que se pretende adicionar entre o valor nenhum e baixo, denominado por muito-baixo, que vai ser avaliado de seguida.

3.4 Proposta de um segundo valor

Analisando os valores relativamente às opções nenhum e baixo, constata-se que a diferença entre estes valores é de 0.22, que é menor que a diferença entre os valores relativos às opções baixo e alto, no entanto pode ajudar a complementar o primeiro critério. Posto isto, na subsecção seguinte vai ser apresentado o mesmo estudo que foi efetuado para a escolha do valor numérico médio.

3.4.1 Métrica Base - Análise das métricas em concordância com os critérios definidos

Foram efetuados os mesmos cálculos agora considerando o intervalo entre]0,0.21] para a determinação do valor muito-baixo.

É de salientar que o cálculo das combinações e os resultados das colisões já consideram o novo valor proposto, o médio.

Como é possível observar na figura 3.6, os resultados são bastante mais satisfatórios dado que conseguimos valores mais próximos do valor máximo da escala, 101. Não é possível obter o valor máximo da escala mas obtivemos valores aproximados, com uma melhoria significativa comparativamente aos valores por omissão e também ao valor médio. O único valor que se obtém uma maior diversidade de classificações é o 0.01, todavia este valor está muito próximo do valor nenhum. Relativamente às métricas referentes à percentagem de valores nas classificações alta e crítica, estão todos abaixo dos valores por omissão e o mesmo acontece para a curtose nas classificações elevadas e no total.

No que diz respeito ao primeiro critério, os valores a ter em consideração serão os mais próximos de 101, que neste caso são os valores [0.01,0.07], que estão a um máximo de 5 valores de distância. Na tabela 3.5 identifica-se que os valores com a curtose nas

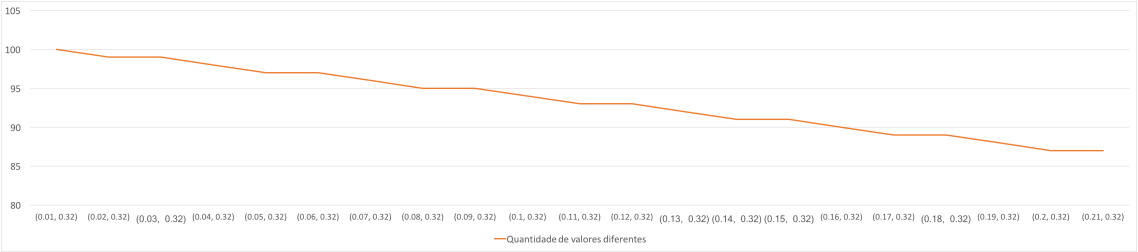

Figura 3.6: Contabilização de *Scores* da métrica base com cinco valores na sub-métrica impacto

classificações alta e crítica mais favoráveis são o 0.06 e o 0.04, uma vez que na curtose alta o valor 0.06 tem o valor mais baixo, -0.93 e na curtose crítica o valor 0.04 tem o valor mais baixo, -2.16. Visto que na curtose geral o valor mais satisfatório é o 0.04, o que representa uma distribuição mais homogénea em todas as classificações, este é o valor escolhido considerando apenas a métrica base.

Neste sentido, de seguida vai ser apresentada a mesma análise para a métrica ambiental, de modo a validar se o valor 0.04 também é o mais favorável.

Métrica Base	Valor Médio	%Nenhum [0]	%Baixo [0.1,4)	%Médio [4,7)	%Alto [7,9)	%Critico [9,10]	Curtose Alta	Curtose Crítica	Curtose Total
	0.01	3.2	23.3	56.9	15.3	1.4	-0.76	-1.59	-0.78
	0.02	2.0	24.2	57.0	15.4	1.4	-0.51	-1.39	-1.26
	0.03	0.8	24.8	57.3	15.7	1.4	-0.53	-1.83	-1.26
	0.04	0.8	24.5	57.4	15.8	1.4	-0.52	-2.16	-1.27
	0.05	0.8	23.9	58.0	15.8	1.5	-0.91	-1.15	-1.19
	0.06	0.8	23.3	58.5	15.9	1.5	-0.93	-1.41	-1.20
	0.07	0.8	22.8	58.8	16.1	1.5	-0.75	-0.65	-1.14
	0.08	0.8	22.4	59.1	16.2	1.5	-1.14	-1.35	-1.20
	0.09	0.8	21.8	59.4	16.6	1.5	-0.87	-0.75	-1.28
	0.10	0.8	21.1	59.8	16.9	1.5	0.18	-0.75	-1.22
5 valores	0.11	0.8	20.6	60.2	16.8	1.5	-0.54	-1.97	-1.18
	0.12	0.8	20.0	60.7	17.0	1.5	-1.19	-1.74	-1.16
	0.13	0.8	19.5	61.0	17.1	1.5	-1.23	-1.70	-1.10
	0.14	0.8	19.0	61.4	17.2	1.5	-1.21	-1.21	-1.24
	0.15	0.8	18.3	61.9	17.5	1.5	-1.22	-1.62	-1.29
	0.16	0.8	17.6	62.4	17.6	1.6	-1.17	-2.06	-1.28
	0.17	0.8	17.2	62.7	17.7	1.6	-1.11	-1.83	-1.26
	0.18	0.8	16.3	63.3	17.9	1.7	-0.81	-0.80	-1.25
	0.19	0.8	15.8	63.3	18.3	1.7	-0.39	-0.43	-1.23
	0.20	0.8	15.3	63.7	18.4	1.8	-0.57	-0.04	-1.22
	0.21	0.8	14.7	63.9	18.9	1.8	-0.26	-1.48	-1.07
3 valores	-	3.7	16.0	56.5	21.4	2.4	1,33	1,13	0,09

Tabela 3.5: Métricas para a escolha do quinto valor - Métrica Base - percentagem de valores nas classificações qualitativas e Curtose

3.4.2 Métrica Ambiental - Análise das métricas em concordância com os critérios definidos

Como indicado, foi repetido o processo para o cálculo das combinações e respetivas colisões, como também as métricas que auxiliam na escolha do valor muito-baixo (Tabela 3.6). Novamente, a distribuição de classificações é bastante mais favorável, com um máximo de 7 valores a mais comparativamente aos valores por omissão conjugado com o valor médio (Figura 3.7). A quantidade de valores nas classificações alta e crítica é menor

em todos os valores numéricos comparativamente aos valores por omissão. Já os valores na curtose crítica não são os mais favoráveis dado que os melhores estão muito próximos do valor numérico 0, que equivale ao valor nenhum, ou então estão muito distantes do valor de distribuição mais apelativo - maior que 95. Como tal, tendo em consideração a análise efetuada anteriormente, não existe um valor que se destaque mais que os outros e por este motivo o valor numérico para o muito-baixo é o 0.04, já que obtivemos métricas coerentes com os critérios definidos na métrica base.

Métrica Base	Valor Muito-Baixo	%Nenhum [0]	%Baixo [0.1,4)	%Médio [4,7)	%Alto [7,9)	%Critico [9,10]	Curtose Alta	Curtose Crítica	Curtose Total
5 valores	0.01	3.3	26.8	50.7	17.2	2.1	-1.20	-0.64	-0.29
	0.02	1.8	27.8	51.1	17.3	2.1	-1.21	-0.21	-1.49
	0.03	1.1	28.1	51.4	17.4	2.1	-1.12	0.21	-1.47
	0.04	1.1	27.5	51.8	17.5	2.1	-1.07	0.68	-1.48
	0.05	1.1	27.1	52.1	17.6	2.1	-1.08	0.60	-1.48
	0.06	0.8	26.8	52.6	17.6	2.2	-1.09	0.42	-1.49
	0.07	0.8	26.3	53.0	17.8	2.2	-1.08	0.42	-1.49
	0.08	0.8	25.7	53.4	17.9	2.2	-1.10	0.34	-1.51
	0.09	0.8	25.2	53.8	18.0	2.2	-1.12	0.19	-1.51
	0.10	0.8	24.5	54.3	18.2	2.2	-1.05	0.05	-1.51
	0.11	0.8	23.9	54.8	18.2	2.2	-1.02	0.17	-1.53
	0.12	0.8	23.3	55.2	18.4	2.2	-1.05	0.16	-1.51
	0.13	0.8	22.8	55.5	18.6	2.3	-0.97	0.34	-1.52
	0.14	0.8	22.1	56.1	18.7	2.3	-1.11	-0.32	-1.52
	0.15	0.8	21.5	56.5	18.9	2.3	-1.16	-0.42	-1.53
	0.16	0.8	20.9	57.0	19.0	2.3	-1.20	-0.20	-1.54
	0.17	0.8	20.3	57.3	19.2	2.3	-1.13	0.18	-1.54
	0.18	0.8	19.7	57.8	19.4	2.3	-1.09	0.23	-1.53
	0.19	0.8	19.1	58.1	19.7	2.4	-1.04	0.42	-1.53
	0.20	0.8	18.5	58.4	19.9	2.4	-1.03	0.71	-1.53
	0.21	0.8	17.9	58.7	20.1	2.4	-0.91	0.03	-1.50
3 valores	-	3.7	20.1	49.7	23.3	3.2	-0,91	-0,26	0,57

Tabela 3.6: Métricas para a escolha do quinto valor - Métrica Ambiental - percentagem de valores nas classificações e Curtose

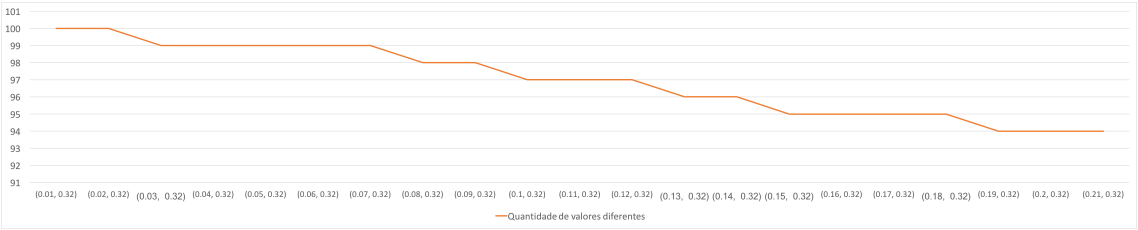

Figura 3.7: Contabilização de *Scores* da métrica ambiental com cinco valores na sub-métrica impacto

Com os novos valores, médio e muito-baixo, verifica-se uma distribuição mais homogénea tanto em toda a escala como na escala qualitativa alta e crítica comparativamente aos valores por omissão do CVSS.

As figuras 3.8 e 3.9 permitem identificar as melhorias da extensão proposta, dado que o número de colisões no valor 0 é bastante menor, existem mais valores na escala e existem muito menos picos, ou seja, menos colisões comparativamente ao CVSS versão 3. Deste modo, comprovou-se que cumpre com o primeiro objetivo apresentado.

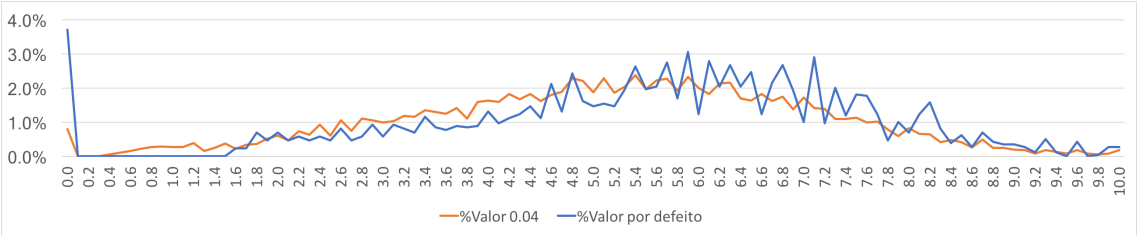

Figura 3.8: Distribuição de valores em proporção - Métrica Base com os 3 valores por defeito e os novos valores

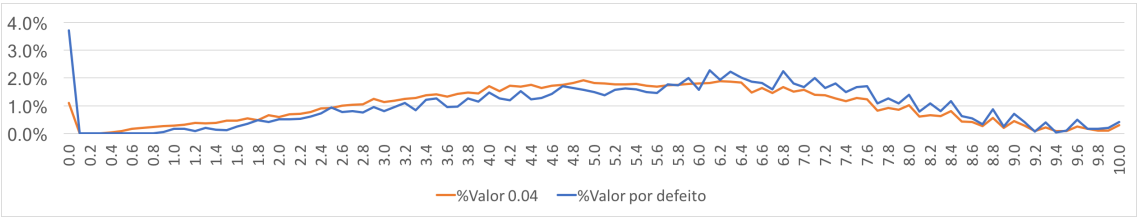

Figura 3.9: Distribuição de valores em proporção - Métrica Ambiental com os 3 valores por defeito e os novos valores

À semelhança do exposto anteriormente, as figuras 3.10, 3.11, 3.12 e 3.13 permitem identificar o cumprimento do segundo objetivo, na medida em que se verifica uma diminuição considerável de valores nas classificações alta e crítica comparativamente aos valores por omissão no CVSS. Para além disso, a distribuição de valores tanto na classificação alta como crítica é mais homogénea.

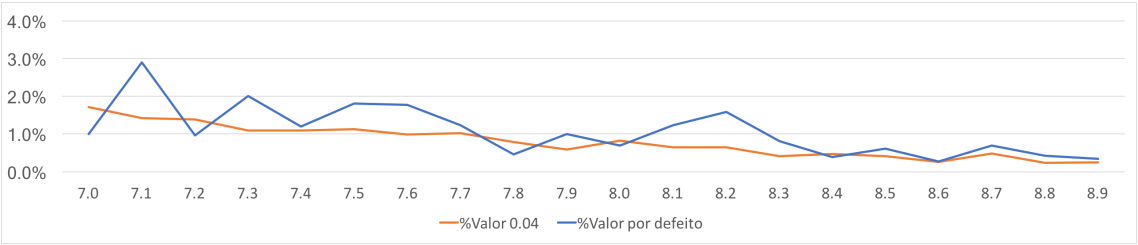

Figura 3.10: Distribuição de valores na classificação alta em proporção - Métrica Base com os novos valores e os por omissão

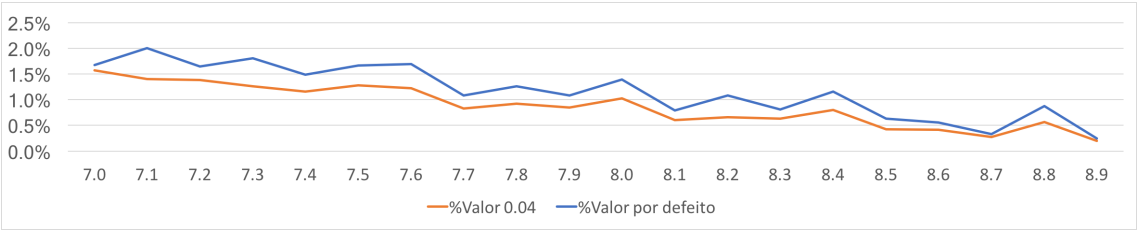

Figura 3.11: Distribuição de valores na classificação alta em proporção - Métrica Ambiental com os novos valores e os por omissão

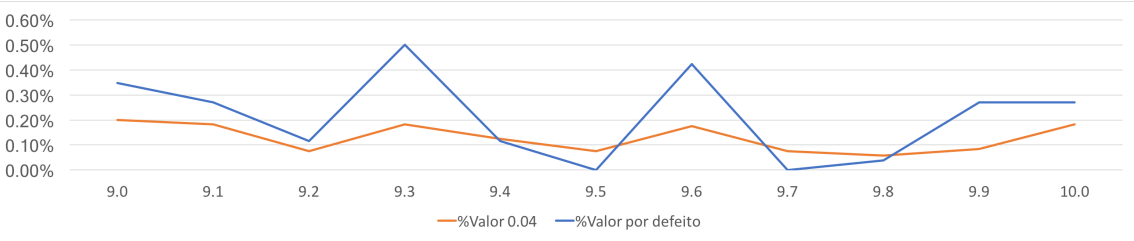

Figura 3.12: Distribuição de valores na classificação crítica em proporção - Métrica Base com os novos valores e os por defeito

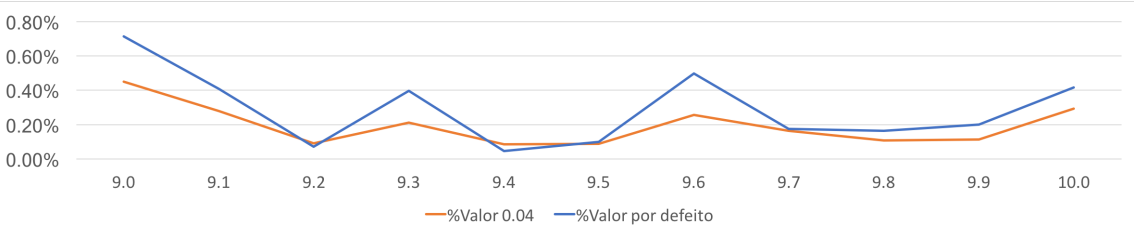

Figura 3.13: Distribuição de valores na classificação crítica em proporção - Métrica Ambiental com os novos valores e os por defeito

Deste modo é acrescentado aos três impactos da métrica base mais um valor, como representado na tabela 3.7.

Opção	Valor
Alto	0.56
Médio	0.32
Baixo	0.22
Muito-Baixo	0.04
Nenhum	0

Tabela 3.7: Métrica Base - Impacto na confidencialidade, integridade e disponibilidade

3.5 Definição dos novos valores

Foram propostos dois novos valores para a sub-métrica de impacto da métrica base, o valor médio e muito-baixo.

Os valores referentes ao impacto na confidencialidade, integridade e disponibilidade foram definidos no CVSS versão 3 da seguinte forma:

Impacto na confidencialidade

1. Alto: Existe uma perda total de confidencialidade, resultando em todos os recursos dentro do componente impactado obtidos pelo atacante. Alternativamente, o acesso

a apenas algumas informações restritas é obtido, mas a informação divulgada apresenta um impacto direto e crítico. Por exemplo, um atacante rouba a senha do administrador ou chave de criptografia privada de um servidor web.

2. Baixo: Existe alguma perda de confidencialidade. O acesso a algumas informações restritas é obtido, mas o atacante não tem controlo sobre as informações que obtem, ou a quantidade ou tipo de perda. A divulgação de informações não causa uma perda direta e crítica para o componente impactado.

3. Nenhum: Não há perda de confidencialidade dentro do componente impactado.

Impacto na integridade

1. Alto: Existe uma perda total de integridade ou uma completa perda de proteção. Por exemplo, o atacante pode modificar qualquer/todos os ficheiros protegidos pelo componente impactado. Alternativamente, apenas alguns ficheiros podem ser modificados, mas as modificações maliciosas apresentam uma consequência direta e crítica para o componente impactado.

2. Baixo: A modificação de dados é possível, mas o atacante não tem controlo sobre a consequência de uma modificação, ou a quantidade de modificações possíveis. A modificação de dados não tem um impacto direto e crítico sobre o componente impactado.

3. Nenhum: Não há perda de integridade dentro do componente impactado.

Impacto na disponibilidade

1. Alto: Existe uma perda total de disponibilidade, em que o atacante pode negar completamente o acesso aos recursos no componente impactado; Essa perda é sustentada (enquanto o atacante continua a executar o ataque) ou persistente (a condição persiste mesmo após o ataque ter concluído). Alternativamente, o atacante tem a capacidade de negar alguma disponibilidade, mas a perda de disponibilidade apresenta uma consequência direta e crítica para o componente impactado (por exemplo, o atacante não pode interromper ligações existentes, mas pode evitar novas ligações; o atacante pode explorar repetidamente uma vulnerabilidade que, em cada instância de um ataque bem-sucedido, perde uma pequena quantidade de memória, mas após a exploração repetida provoca a indisponibilidade total de um serviço).

2. Baixo: Há uma redução de desempenho ou interrupções na disponibilidade de recursos. Mesmo que a exploração repetida da vulnerabilidade seja possível, o atacante não tem a capacidade de negar completamente o serviço aos utilizadores legítimos. Os recursos no componente impactado estão parcialmente disponíveis o tempo todo, ou totalmente disponíveis apenas algumas vezes, mas, em geral, não existe nenhuma consequência direta e crítica para o componente impactado.

3. Nenhum: Não há impacto na disponibilidade no componente impactado.

Com a proposta de melhoria ao CVSS versão 3, as definições indicadas anteriormente já não fazem sentido considerando os novos dois valores, muito-baixo e médio.

Atendendo às propostas disponibilizadas por entidades com experiência e conhecimento na área de segurança [6] para melhorar o CVSS versão 2, já indicadas no capítulo 2.6, e considerando as definições indicadas anteriormente, estas foram ligeiramente alteradas e adaptadas com a definição dos novos valores propostos, que vão ser seguidamente apresentados:

Impacto na confidencialidade

1. Alto: Existe uma perda total de confidencialidade, resultando em todos os recursos dentro do componente impactado obtidos pelo atacante. Por exemplo, controlo total do servidor, acesso a toda a informação pessoal dos clientes ou cartões de crédito, chaves privadas, credenciais de administração.

2. Médio: Existe uma grande perda de confidencialidade, em que o acesso a todos os dados na aplicação podem ser divulgados. Por exemplo, acesso a todas as tabelas na base de dados ou comprometer toda a aplicação.

3. Baixo: Existe alguma perda de confidencialidade, em que o acesso a um subconjunto dos dados é obtido, mas o atacante não tem controlo sobre as informações que obtém, ou a quantidade ou tipo de perda. Por exemplo, acesso a uma tabela na base de dados.

4. Muito-Baixo: Existe uma pequena perda de confidencialidade, em que o acesso a algumas informações é obtido, mas a informação ajuda apenas o atacante na identificação de possíveis vulnerabilidades, por exemplo, as versões dos componentes que estão a disponibilizar serviços, nome do servidor, detalhes dos erros com a divulgação do caminho da aplicação, entre outros.

5. Nenhum: Não há perda de confidencialidade dentro do componente impactado.

Impacto na integridade

1. Alto: Existe uma perda total de integridade ou uma completa perda de proteção. Por exemplo, o atacante pode modificar qualquer/todos os ficheiros protegidos pelo componente impactado. Por exemplo, corrupção total das bases de dados do sistema.

2. Médio: Existe uma grande perda de integridade, em que todos os dados acessíveis na aplicação podem ser modificados. Por exemplo, alteração de todas as tabelas numa base de dados.

3. Baixo: Existe alguma perda de integridade, em que um sub-conjunto dos dados na aplicação podem ser manipulados. Por exemplo, alteração de uma tabela na base de dados.

4. Muito-Baixo: A modificação de uma pequena quantidade de dados é possível, mas não tem um impacto direto e crítico sobre o componente impactado. Por exemplo, alteração da resposta de um servidor web para a vítima.

5. Nenhum: Não há perda de integridade dentro do componente impactado.

Impacto na disponibilidade

1. Alto: Existe uma perda total de disponibilidade, em que o atacante pode negar completamente o acesso aos recursos no componente impactado; Essa perda é sustentada (enquanto o atacante continua a executar o ataque) ou persistente (a condição persiste mesmo após o ataque ter concluído).

2. Médio: Existe uma grande perda de disponibilidade, em que é negado o acesso à aplicação até ser efetuado, por exemplo, um *restart/reboot*.

3. Baixo: Existe alguma perda de disponibilidade, em que um sub-conjunto de funcionalidades da aplicação não estão disponíveis ou a aplicação está disponível por um curto espaço de tempo.

4. Muito-Baixo: Existe uma pequena perda de disponibilidade, em que há uma redução de desempenho ou interrupções na disponibilidade de recursos.

5. Nenhum: Não há impacto na disponibilidade no componente impactado.

É de salientar que no caso de obtenção ou manipulação de dados pessoais na exploração bem-sucedida de uma vulnerabilidade, o valor definido para o impacto na confidencialidade e integridade é alto, isto porque as repercussões que advém do roubo ou manipulação desse tipo de informação são bastantes elevadas dado o incumprimento ao regulamento geral da proteção de dados (RGPD) [41].

3.6 Resumo

Neste capítulo foram discutidos os dois problemas do CVSS versão 3, relativamente à grande quantidade de vulnerabilidades nas classificações alta e crítica e diversidade de valores.

Deste modo, os critérios para a extensão de melhoria do CVSS foram definidos tendo em consideração os problemas indicados. Neste sentido, foram propostos dois novos valores, o médio e o muito-baixo e através de um conjunto de métricas foram escolhidos

os dois valores numéricos correspondentes, 0.32 e 0.04 respetivamente. Como tal, foi comparada a distribuição de valores em proporção entre estes valores e os por omissão do CVSS versão 3. Neste sentido, identificou-se um aumento significativo na diversidade de valores em toda a escala e uma diminuição de valores críticos e altos.

Por fim, os valores da sub-métrica de impacto foram redefinidos em concordância com as propostas efetuadas por entidades experientes em Segurança e as próprias definições disponibilizadas pelo FIRST.

Capítulo 4

Avaliação e resultados

O NVD é um repositório do governo dos Estados Unidos [24] que disponibiliza as vulnerabilidades identificadas em softwares de diversos fabricantes. O NVD é um produto do NIST Computer Security [23], laboratório de tecnologias de informação e é patrocinado pelo *Department of Homeland Security's National Cyber Security Division* [26]. À medida que os fabricantes disponibilizam informação acerca das vulnerabilidades, estas são atualizadas e avaliadas pelo NVD.

Dado que é necessário reavaliar vulnerabilidades que tenham sido avaliadas pelo sistema de avaliação de vulnerabilidades CVSS versão 3 apenas com a métrica obrigatória, sendo esta, a métrica base, considerou-se esta base de dados de vulnerabilidades para efetuar a validação da proposta anteriormente apresentada.

Considerando que é necessário efetuar a mesma validação mas para vulnerabilidades em que são conhecidos os requisitos na confidencialidade, integridade e disponibilidade do ativo, através de uma parceria com a EDP, é utilizada uma amostra de vulnerabilidades reais disponibilizadas pelo mesmo.

A validação consiste em reavaliar as primeiras 100 vulnerabilidades classificadas como críticas referentes a Dezembro de 2017 (Tabela A.1) e as primeiras 100 vulnerabilidades classificadas como altas entre 1 de Janeiro e 31 de Dezembro de 2017 (Tabela A.2). Como as vulnerabilidades do Grupo EDP estão classificadas qualitativamente e o sistema de avaliação é diferente do CVSS, estas vulnerabilidades são avaliadas numa primeira fase com os valores por omissão do CVSS versão 3 e numa segunda fase reavaliadas considerando os novos valores propostos (Tabelas A.3, A.4, A.5, A.6, A.7 e A.8).

4.1 Vulnerabilidades NVD

Nas próximas subseções vão ser apresentadas as avaliações e respetivos resultados considerando 100 vulnerabilidades pertencentes à classificação crítica e 100 vulnerabilidades pertencentes à classificação alta. Esta amostra é disponibilizada pelo NVD.

4.1.1 Classificação crítica

A avaliação das 100 primeiras vulnerabilidades de Dezembro de 2017 com classificação crítica (Tabela A.1) foram reavaliadas tendo em consideração a nova definição dos valores nenhum, muito-baixo, baixo, médio e alto da sub-métrica de impacto da métrica base. Destas vulnerabilidades 95% são classificadas com o valor quantitativo 9.8 (Figura 4.1).

Após a reavaliação destas vulnerabilidades, identificou-se uma redução de 32% na classificação quantitativa 9.8. Considerando que apenas existe uma combinação possível para obter a classificação 9.8, sendo esta a seguinte:

- Superfície de ataque: Rede
- Complexidade do ataque: Baixo
- Privilégios Requeridos: Nenhum
- Interação do utilizador: Nenhum
- Âmbito: Não altera
- Impacto na confidencialidade: Alto
- Impacto na integridade: Alto
- Impacto na disponibilidade: Alto

E diminuindo os impactos na confidencialidade, integridade e disponibilidade, para um valor médio, dois valores médios ou três valores médios, obtém-se os valores 9.5, 9.1 e 8.3. Na reavaliação estes valores são refletidos, com 5% no 9.5, 12% no 9.1 e 18% no 8.3 (Figura 4.1 e 4.2). Considerando que a classificação quantitativa 8.3 corresponde à classificação qualitativa alta, é desta forma evidenciado que com o novo valor médio foi possível reduzir o número de colisões como também baixar o nível de severidade para o valor qualitativo alto. É de realçar que não era possível obter o valor 9.5 na métrica base com os valores por omissão do CVSS versão 3. Pelos resultados obtidos, 5% das vulnerabilidades foram classificadas com este valor, o que significa que existiu um aumento na distribuição de valores. Assim é possível evitar tantas colisões em determinados valores como no caso do valor 9.8.

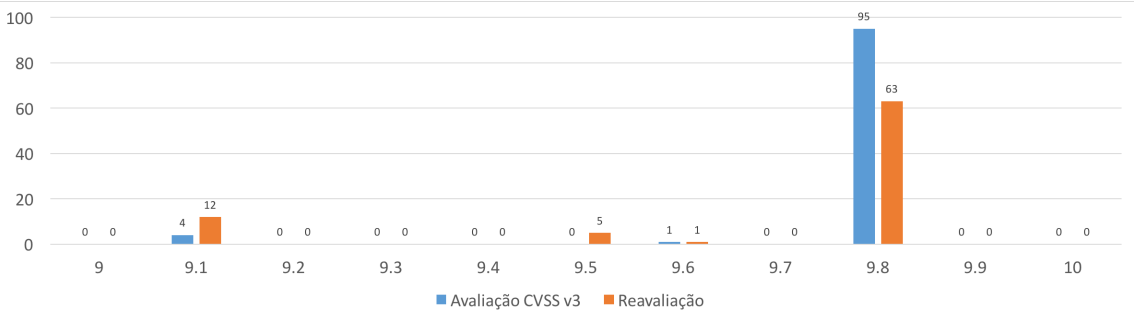

Figura 4.1: Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - NVD

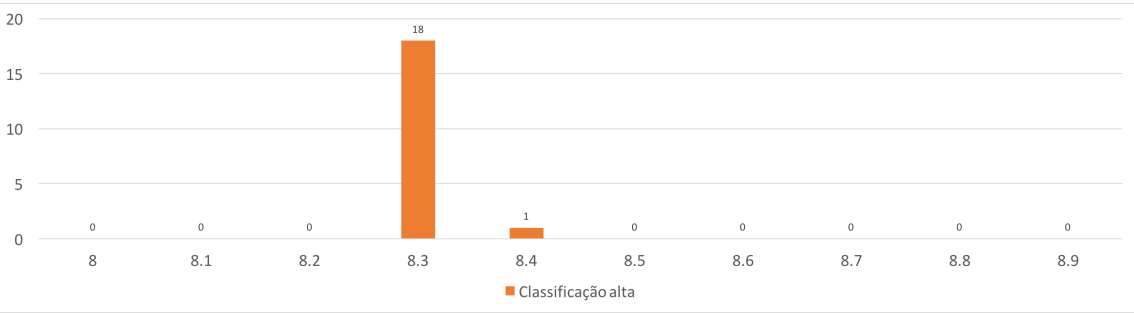

Figura 4.2: Diminuição da classificação crítica para valores da classificação alta - NVD

4.1.2 Classificação alta

De modo a identificar possíveis melhorias à adição do valor muito-baixo, foi efetuada a mesma revisão mas neste caso para vulnerabilidades com severidade alta, em que a confidencialidade, integridade ou disponibilidade continham o valor baixo (Tabela A.2).

Dado que para o mesmo intervalo de tempo apenas existia uma amostragem de 3 vulnerabilidades, o intervalo foi aumentado de um mês, Dezembro, para um ano, de 1 de Janeiro a 31 de Dezembro de 2017. Os valores são mais dispersos do que na classificação crítica, no entanto os valores 7.3 e 8.2 destacam-se relativamente aos restantes valores. Desta forma, foram retiradas as primeiras 34 vulnerabilidades com baixo impacto na confidencialidade, as primeiras 33 vulnerabilidades com baixo impacto na integridade e por fim, as primeiras 33 vulnerabilidades com baixo impacto na disponibilidade.

Obteve-se resultados bastante favoráveis, dado que em 100 vulnerabilidades na classificação alta, existiam 66% de colisões nos valores 8.2 e 7.3 (Figura 4.3) e com a reavaliação este valor diminuiu consideravelmente para os 15%. Para além desta diminuição, constata-se que 38% das vulnerabilidades passaram para o nível de severidade médio (Figura 4.4).

Conclui-se assim que com o valor muito-baixo, foi possível diminuir a quantidade de vulnerabilidades com classificação alta.

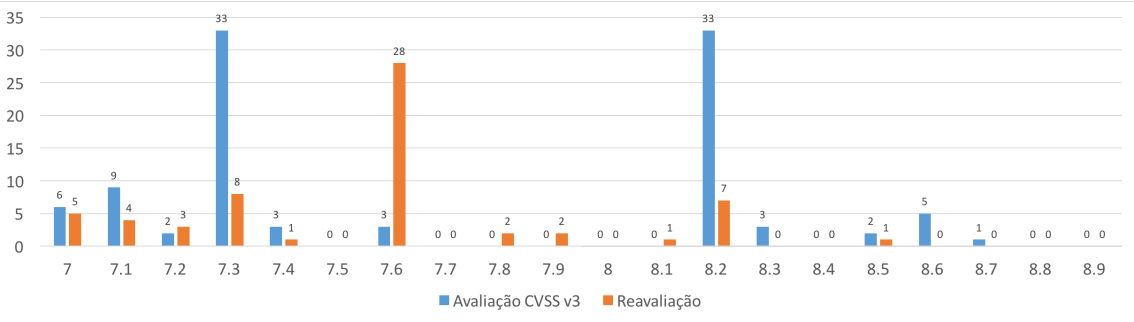

Figura 4.3: Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - NVD

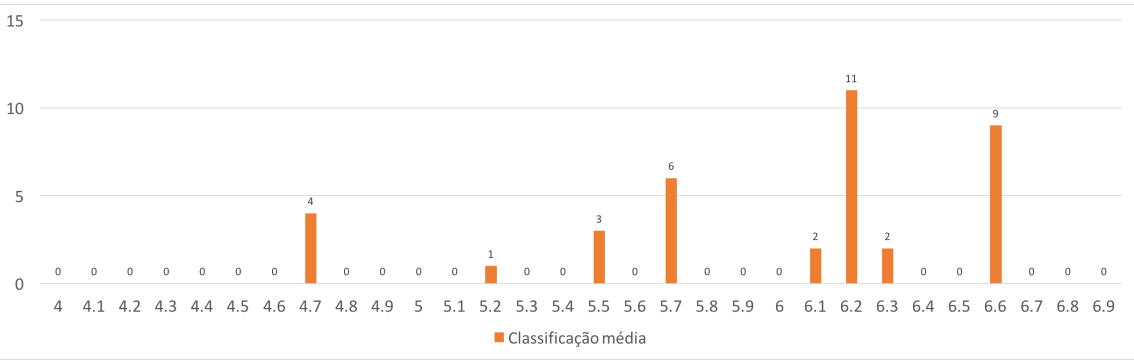

Figura 4.4: Diminuição da classificação alta para valores da classificação média - NVD

Com a utilização da classificação do NVD, que recorre ao sistema de avaliação de vulnerabilidades CVSS versão 3, foi possível identificar melhorias ao mesmo com a adoção da extensão proposta. Este estudo foi apenas efetuado para a métrica base, dado que estas vulnerabilidades são identificadas em software, extensões, *frameworks*, que podem ser utilizadas em qualquer sistema académico ou empresarial. Neste sentido, as vulnerabilidades são apenas classificadas com o intuito de avaliar os fatores inerentes à mesma, utilizando para isso a métrica obrigatória. No entanto, para ser possível avaliar se a proposta apresentada também melhora o sistema de avaliação de vulnerabilidades conhecendo a criticidade do ativo, foi recolhida uma amostra de 200 vulnerabilidades mitigadas do Grupo EDP (Tabelas A.3, A.4, A.5, A.6, A.7 e A.8). Esta análise vai ser mostrada na subsecção seguinte.

4.2 Vulnerabilidade EDP

De modo a efetuar a avaliação das vulnerabilidades reais do Grupo EDP, é necessário ter conhecimento dos requisitos na confidencialidade, integridade e disponibilidade de cada ativo para definir os valores da métrica ambiental. Neste sentido, são apresentados de seguida os quatro níveis de criticidade definidos pelo Grupo EDP para cada ativo:

1. *Diamond*
2. *Gold*
3. *Silver*
4. *Bronze*

Esta classificação é atribuída a cada ativo do Grupo EDP considerando apenas os requisitos na disponibilidade. Como tal, os níveis de criticidade do ativo foram mapeados para os valores do CVSS versão 3 da seguinte forma:

Criticidade do ativo	Requisitos na confidencialidade	Requisitos na integridade	Requisitos na disponibilidade
Diamond	Nenhum	Nenhum	Alto
Gold	Nenhum	Nenhum	Médio
Silver	Nenhum	Nenhum	Médio
Bronze	Nenhum	Nenhum	Baixo

Tabela 4.1: Mapeamento entre a criticidade do ativo e os requisitos na confidencialidade, integridade e disponibilidade

Como tal, foram atribuídos os valores nenhum, baixo, médio e alto referente aos requisitos na confidencialidade, integridade e disponibilidade da métrica ambiental a cada vulnerabilidade consoante o nível de criticidade de cada ativo.

A avaliação que vai ser exposta nas subsecções seguintes foi divida em duas fases: a primeira fase consistiu na avaliação das vulnerabilidades tendo em consideração apenas os valores disponíveis pelo CVSS versão 3 da métrica base e ambiental. Na segunda fase, as 200 vulnerabilidades foram avaliadas novamente atendendo aos novos valores, muito-baixo e médio.

4.2.1 Classificação crítica

Na primeira fase, o valor que se destaca é o 9.5 dado que contém 48% de colisões (Figura 4.5), o que equivale a quase metade das vulnerabilidades avaliadas. Após a reavaliação, este valor diminuiu para menos de metade, com apenas 21% de colisões. À semelhança dos resultados obtidos na reavaliação das vulnerabilidades disponibilizadas no NVD, o nível de severidade de 45% das vulnerabilidades reduziu para o valor qualitativo alto (Figura 4.6). Deste modo, é possível diminuir a quantidade de vulnerabilidades na classificação crítica. Para além do indicado, existem mais seis valores na escala do que existiam com os valores por omissão do CVSS versão 3. Posto isto, comprova-se que a distribuição de valores é maior.

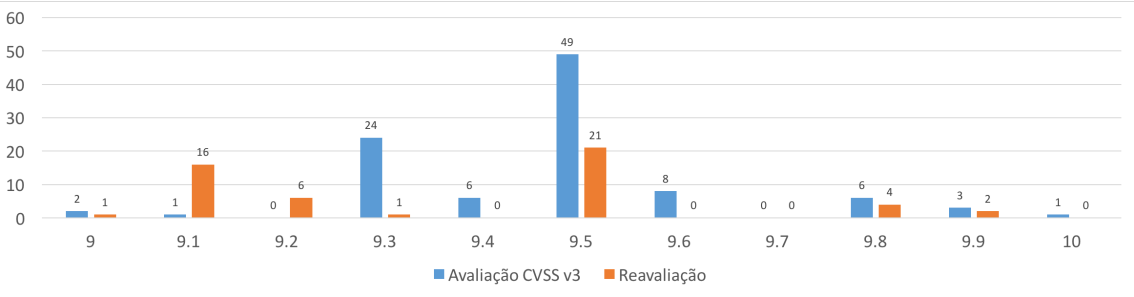

Figura 4.5: Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - EDP

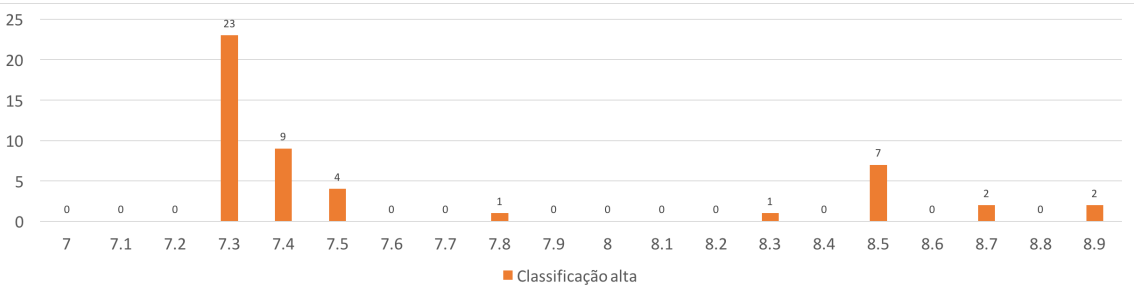

Figura 4.6: Diminuição da classificação crítica para valores da classificação alta - EDP

4.2.2 Classificação alta

O mesmo processo foi efetuado nas 100 vulnerabilidades com severidade alta. O resultado podia ter sido mais satisfatório uma vez que todas as reavaliações anteriores resultaram em reduções de colisões e severidades menores. No entanto, como é possível verificar na figura 4.7, o valor que se destaca é o 8.1, sendo que na reavaliação aumentou 1% das colisões neste valor uma vez que duas vulnerabilidades, uma com 8.2 e outra com 8.3, passaram para a classificação 8.1. Não obstante, é possível aferir que as colisões tanto no valor 8.4 como no valor 7.5 reduziram significativamente e existiram novamente vulnerabilidades a passar da classificação alta para média (Figura 4.8).

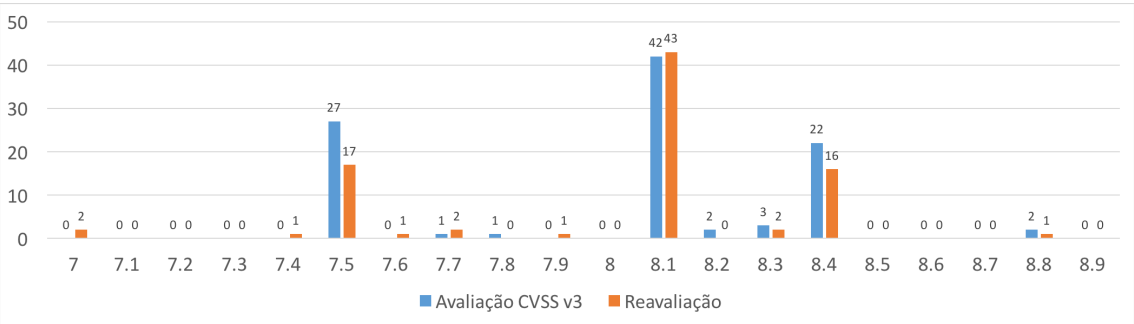

Figura 4.7: Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - EDP

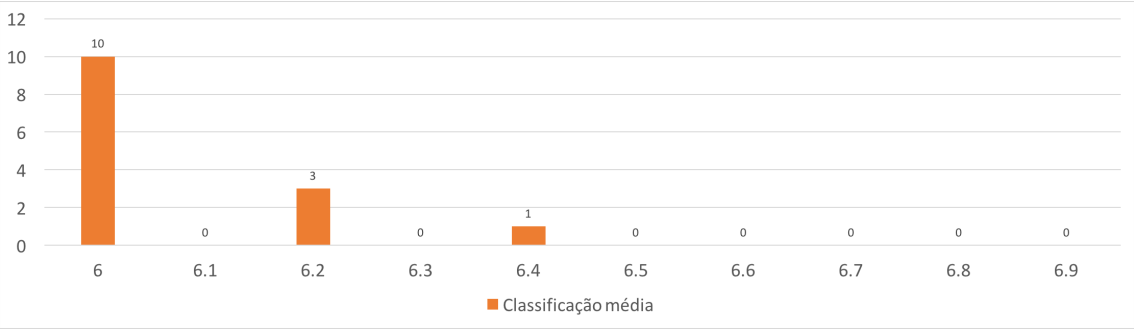

Figura 4.8: Comparação entre os valores por omissão do CVSS versão 3 e a reavaliação das vulnerabilidades com os novos valores propostos - EDP

4.2.3 Comparação dos resultados com a severidade das vulnerabilidades

Os testes de segurança executados no Grupo EDP são contratados a uma empresa externa e a classificação das vulnerabilidades são definidas pela mesma. Esta classificação é qualitativa e os critérios para a avaliação das vulnerabilidades não é publicamente conhecida. Os níveis de classificação atribuídos às vulnerabilidades do Grupo EDP são os seguintes:

1. *Critical*
2. *High*
3. *Medium*
4. *Low*
5. *Info*

As 200 vulnerabilidades avaliadas pelo sistema de avaliação de vulnerabilidades estavam classificadas por esta empresa com os primeiros três níveis de severidade, sendo estes o *Critical*, *High* e *Medium*, com uma percentagem de 45%, 44% e 11% respetivamente (Figura 4.9). No entanto, utilizando a norma, nenhuma desta vulnerabilidades pertence ao nível médio, sendo que 50% das vulnerabilidades pertencem ao nível crítico e 50% ao nível alto (Figura 4.10).

Na reavaliação, as vulnerabilidades sofreram alterações relativamente aos valores quantitativos e qualitativos e por este motivo 7% (Figura 4.11) das 200 vulnerabilidades começaram a pertencer ao nível de classificação médio, menos 4% que o valor atribuído pelo fornecedor. Contudo, a percentagem de vulnerabilidades consideradas críticas pelo fornecedor é maior que na reavaliação, dado que pelos resultados apenas 27% das vulnerabilidades são críticas. É possível verificar que a maioria das vulnerabilidades são classificadas como altas, com 66%, todavia como uma das vantagens do CVSS é a possibilidade de as classificar quantitativamente, o facto de existirem em maior quantidade na

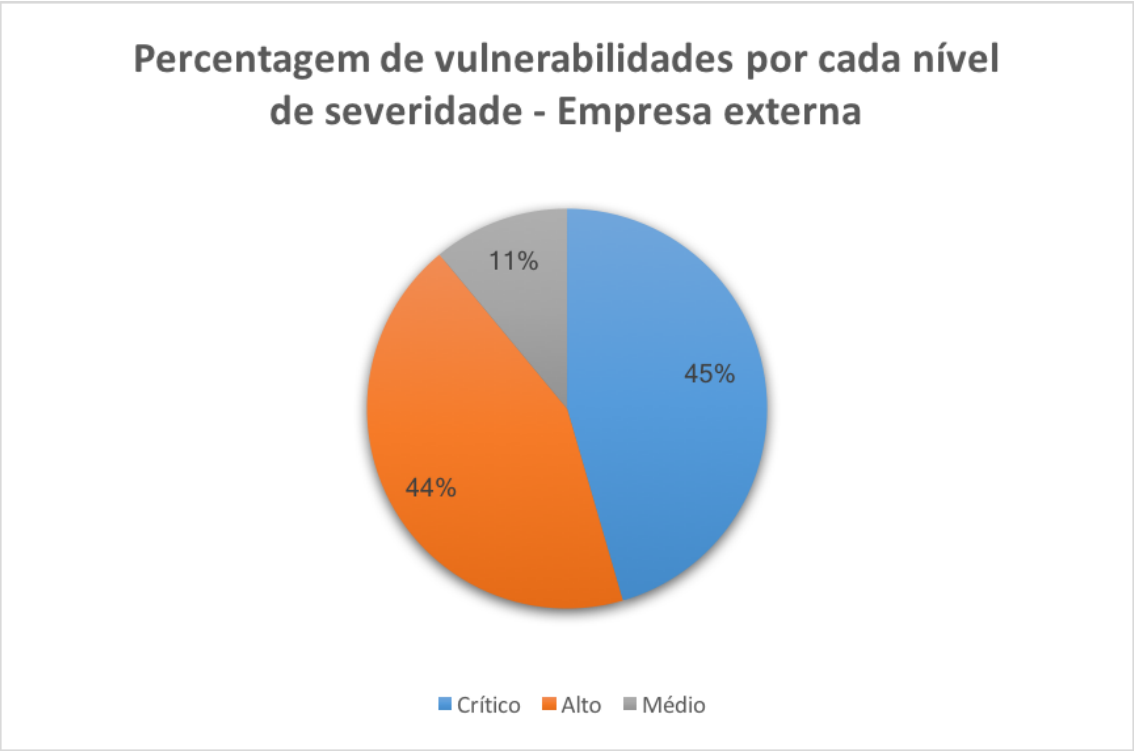

Figura 4.9: Percentagem de vulnerabilidade por cada nível de severidade - Empresa externa

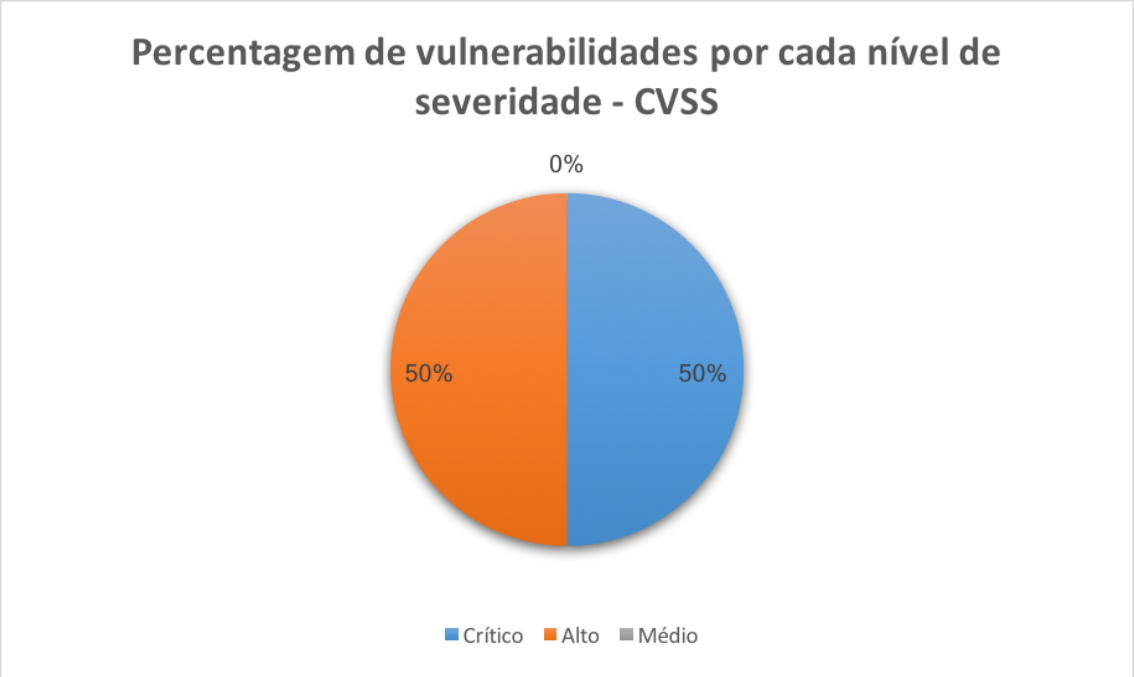

Figura 4.10: Percentagem de vulnerabilidade por cada nível de severidade - CVSS

classificação alta, não acrescenta complexidade na priorização das vulnerabilidades, dado que possuímos os valores quantitativos e estes encontram-se bem distribuídos como já

apresentado anteriormente.

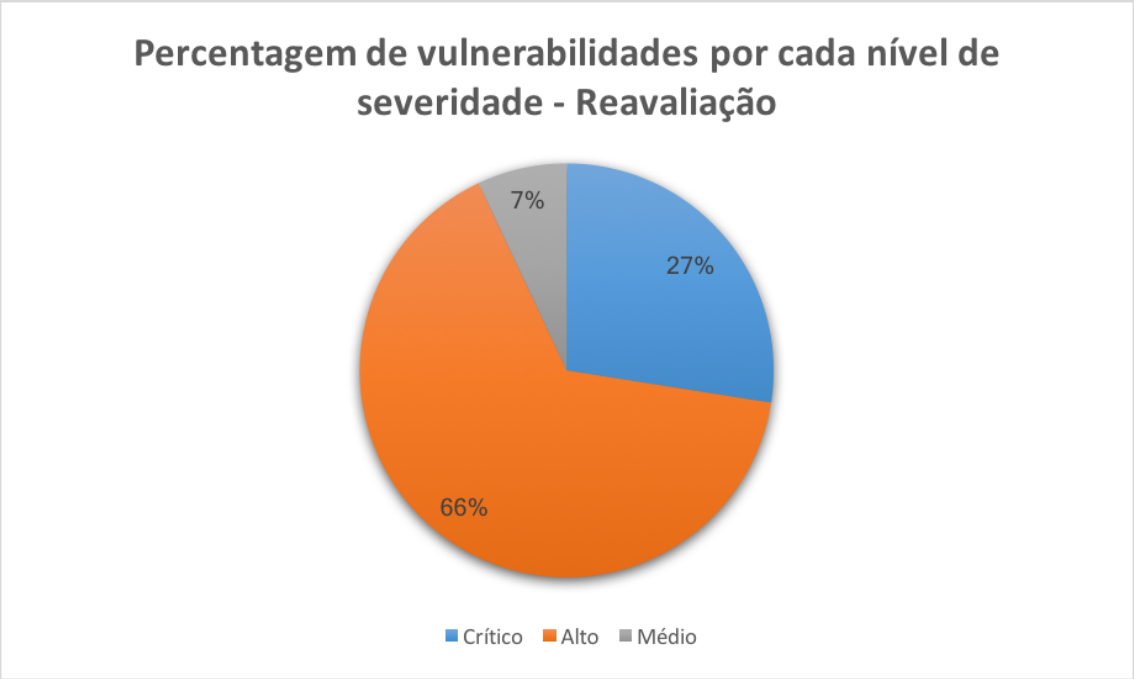

Figura 4.11: Percentagem de colisões por classificação - após reavaliação

Em conclusão, verificou-se que com a extensão de melhoria ao CVSS versão 3 é possível reduzir as colisões em valores com uma grande quantidade de colisões e também reduzir a severidade das vulnerabilidades. Desta forma, comprovou-se que esta proposta cumpre os objetivos delineados inicialmente, considerando que foi possível diminuir o número de vulnerabilidades nas classificações crítica e alta e obteve-se uma distribuição mais homogénea de valores em toda a escala, como exposto no presente capítulo.

4.3 Resumo

Neste capítulo foi apresentado a metodologia utilizada para avaliação da extensão proposta usando amostras de vulnerabilidades do NVD e Grupo EDP. No caso do NVD, esta avaliação foi efetuada a 200 vulnerabilidades, 100 correspondentes à classificação crítica e 100 referentes à classificação alta. Estas vulnerabilidades foram reavaliadas considerando os novos valores propostos, muito-baixo e médio. As vulnerabilidades do Grupo EDP foram avaliadas primeiramente com os valores por omissão do CVSS e posteriormente reavaliadas com a extensão de melhoria proposta.

Na reavaliação das vulnerabilidades publicadas no NVD com a classificação do CVSS comprovou-se que é possível reduzir a quantidade de colisões em classificações quantitativas com elevadas colisões, como no caso do valor 9.8, que tinha 95% de colisões e após a reavaliação passou a ter 63%. Isto deve-se também ao valor 9.5, que ficou com 5% das

vulnerabilidades classificadas com 9.8. Dado que o valor 9.5 não se obtinha na avaliação das vulnerabilidades com os valores por omissão constata-se a importância da obtenção do maior número possível de valores na escala, sem este valor teríamos mais colisões no valor 9.8. Também se verificou uma redução de vulnerabilidades na classificação crítica e alta, dado que com a inserção dos novos valores foi possível passar algumas vulnerabilidades de severidade crítica para alta e de alta para média.

Na validação das 200 vulnerabilidades no Grupo EDP, também se identificou melhorias tanto na redução de colisões por classificação quantitativa como qualitativa. Em comparação com as classificações atribuídas pela empresa de execução de testes de segurança verificou-se uma grande discrepância nas classificações comparativamente ao atual sistema de avaliação de vulnerabilidades CVSS. Posto isto, a adoção de uma diferente metodologia para avaliação das vulnerabilidades e tendo como pressuposto que não existe conhecimento do negócio da empresa e nível de criticidade dos ativos, é expetável que estes valores não estejam alinhados com o CVSS. Não obstante, é uma boa prática a adoção de uma norma utilizada por enumeras entidades dado que assim é mais fácil a comunicação entre as partes.

Capítulo 5

Conclusão e Trabalho futuro

5.1 Conclusão

Neste trabalho foi apresentado o CVSS, o sistema de avaliação da severidade das vulnerabilidades mais conhecido e adotado por várias entidades reputadas. Foram identificados alguns problemas na versão 3, relativos à grande quantidade de classificações crítica e alta e pouca diversidade de valores. Como tal, foi proposta uma extensão de melhoria ao CVSS versão 3, com o objetivo de reduzir o número de vulnerabilidades nas classificações alta e crítica e aumentar a diversidade de valores. Através da avaliação da solução proposta, considerando 400 vulnerabilidades, 200 do NVD e 200 do Grupo EDP, comprovou-se que os critérios definidos inicialmente foram cumpridos, visto que houve um acréscimo de valores possíveis na escala [0,10] e devido a este facto existiu uma redução de colisões em cada classificação dado o aumento na quantidade de possibilidades. Para além do exposto anteriormente, verificou-se uma redução significativa no número de vulnerabilidades nas classificações crítica e alta, o que está em conformidade com o segundo critério definido.

5.2 Trabalho futuro

Como trabalho futuro, deviam de ser considerados as seguintes melhorias:

- Inserção de mais granularidade aos fatores, como por exemplo, a complexidade do ataque uma vez que o ataque apenas pode ter complexidade baixa ou alta. Por este motivo é que a maioria dos ataques são classificados com complexidade baixa [6].
- Alteração de valores numéricos iguais em diferentes valores da métrica base ou a alteração da fórmula para que seja evitada a atribuição da mesma classificação a vulnerabilidades com fatores diferentes. Como exemplo, uma vulnerabilidade com a string CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L é pontuada da mesma forma que uma vulnerabilidade com a string

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L. Isto acontece dado que foram atribuídos valores numéricos iguais na sub-métrica exploração, que é constituída pela superfície de ataque, complexidade do ataque, privilégios requeridos e interação do utilizador e a fórmula para esta métrica é apenas um produto entre estes fatores, ou seja, multiplicar 8.22 * 0.85 * 0.77 * 0.85 * 0.62 ou multiplicar 8.22 * 0.62 * 0.77 * 0.85 * 0.85 obtém-se o mesmo resultado mesmo que num caso seja possível explorar a vulnerabilidade remotamente mas é necessário ter interação do utilizador e no outro caso é necessário estar no perímetro da organização, ou até mesmo dentro da mesma para aceder ao equipamento de rede.

No decorrer desta dissertação, o FIRST [7] recebeu várias propostas de melhoria ao CVSS versão 3 e foi publicada, no dia 26 de Janeiro de 2018, a lista de possíveis melhorias e as que já foram aceites para a versão 4 do CVSS [12]. Como é possível verificar nesta lista, existem várias melhorias identificadas que podem aumentar o nível de maturidade desta norma.

Bibliografia

[1] E. Byres, A. Ginter, and J. Langill. How stuxnet spreads – a study of infection paths in best practice systems. https://www.tofinosecurity.com/how-stuxnet-spreads, 2011. [Consult. 20 Set. 2016].

[2] CERT/CC. About us. https://www.cert.org/about/. [Consult. 11 Dec. 2017.

[3] CVE. Security vulnerabilities published in 1999. [Consult. 20 Set. 2016].

[4] CVE. Security vulnerabilities published in 2017. https://www.cvedetails.com/vulnerability-list/year-2017/vulnerabilities.html. [Consult. 20 Set. 2016].

[5] CVE. Vulnerability details : Cve-2017-0144 (2 metasploit modules). https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-0144. [Consult. 20 Set. 2017].

[6] C. Eiram and B. Martin. The cvssv2 shortcomings, faults, and failures formulation. https://www.riskbasedsecurity.com/reports/CVSS-ShortcomingsFaultsandFailures.pdf. [Consult. 14 Julho 2018].

[7] FIRST. First is the global forum for incident response and security teams. https://www.first.org/. [Consult. 2 Jan. 2016].

[8] FIRST-SIG. Cvss v3.0 preview 2 - metrics/vector string. https://www.first.org/_assets/downloads/cvss/cvss-v30-preview2-metricvectorstring-december-2014.pdf, 2014. [Consult. 2 Jan. 2016].

[9] FIRST-SIG. Cvss v3.0 preview 2 – formula. https://www.first.org/_assets/downloads/cvss/cvss-v30-preview2-formula-december-2014.pdf, 2014. [Consult. 2 Jan. 2016].

[10] FIRST-SIG. Common vulnerability scoring system v3.0: User guide. https://www.first.org/cvss/user-guide, 2015. [Consult. 10 Set. 2017].

[11] FIRST-SIG. Common vulnerability scoring system v3.0: Examples. https://www.first.org/cvss/cvss-v30-examples_v1.5.pdf, 2017. [Consult. 30 Set. 2018].

[12] FIRST-SIG. List of potential future cvss improvements. https://www.first.org/cvss/workitems, 2018. [Consult. 12 Maio. 2018].

[13] Q. Liu and Y. Zhang. Vrss: A new system for rating and scoring vulnerabilities. *Computer Communications*, 34(3):264–273, 2011.

[14] Q. Liu, Y. Zhang, Y. Kong, and Q. Wu. Improving vrss-based vulnerability prioritization using analytic hierarchy process. *Journal of Systems and Software*, 85(8):1699–1708, 2012.

[15] B. Martin and S. Coley. Common weakness scoring system. https://cwe.mitre.org/cwss/cwss_v1.0.1.html, 2014. Consult. 2 Jan. 2016.

[16] P. Mell and K. Scarfone. Cvss-sig version 2 history. https://www.first.org/cvss/v2/history, Junho 2007. [Consult. 18 Set. 2017].

[17] P. Mell and K. Scarfone. Improving the common vulnerability scoring system. *IET Information Security*, 1(3):119–127, 2007.

[18] P. Mell, K. Scarfone, and S. Romanosky. A complete guide to the common vulnerability scoring system version 2.0. https://www.first.org/cvss/cvss-v2-guide.pdf, Junho 2007. [Consult. 2 Jan. 2016].

[19] P. Mell, K. Scarfone, and Romanosky S. Common vulnerability scoring system. *IIEEE Security & Privacy*, 4(6):85–89, 2006.

[20] MITRE. Corporate overview. https://www.mitre.org/about/corporate-overview. [Consult. 11 Dec. 2017].

[21] MITRE. About cwe. https://cwe.mitre.org/about/index.html, Maio 2017. [Consult. 26 Ago. 2017].

[22] NIAC-FIRST. Common vulnerability scoring system v1 archive. https://www.first.org/cvss/v1/, 2014. [Consult. 10 Fev. 2016].

[23] NIST. About nist. https://www.nist.gov/about-nist. [Consult. 11 Dec. 2017].

[24] NIST. National vulnerability database (nvd). https://nvd.nist.gov/cpe.cfm. [Consult. 2 Jan. 2016].

[25] NIST. Statistics-2016/2017. https://nvd.nist.gov/vuln/search/statistics?adv_search=true&form_type=advanced&results_type=statistics&pub_date_start_month=0&pub_date_start_year=2016&pub_date_end_month=10&pub_date_end_year=2017. [Consult. 11 Nov. 2017].

[26] The Department of Homeland Security. About dhs. https://www.dhs.gov/about-dhs, Setembro 2017.

[27] ORACLE. Use of common vulnerability scoring system (cvss) by oracle. https://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html, Outubro 2017. [Consult. 10 Set. 2017].

[28] OWASP. About the open web application security project. https://www.owasp.org/index.php/About_OWASP. [Consult. 17 Set. 2017].

[29] OWASP. Owasp top ten project. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#OWASP_Top_10_for_2013, 2013. [Consult. 2 Setembro. 2017].

[30] OWASP. Membership. https://www.owasp.org/index.php/Membership#tab=Corporate_Supporters, 2015. [Consult. 30 Agosto. 2017].

[31] OWASP. Owasp risk rating methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 2016. [Consult. 17 Set. 2017].

[32] OWASP. Owasp top 10. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf, 2017. [Consult. 12 Maio. 2018].

[33] RBS. Cvss – is 3 the magic number? https://www.riskbasedsecurity.com/2017/06/cvss-is-3-the-magic-number, Junho 2017. [Consult. 10 Set. 2017].

[34] RBS. Cvss – is version 3 all bad? https://www.riskbasedsecurity.com/2017/05/cvss-is-version-3-all-bad/, Maio 2017. [Consult. 10 Set. 2017].

[35] RBS. Cvssv3: New system, new problems (file-based attacks). https://www.riskbasedsecurity.com/2017/01/cvssv3-new-system-new-problems-file-based-attacks/, Janeiro 2017. [Consult. 10 Set. 2017].

[36] RBS. Cvssv3: New system, next problem (exploit reliability). https://www.riskbasedsecurity.com/2017/01/cvssv3-new-system-next-problem-exploit-reliability/, Janeiro 2017. [Consult. 10 Set. 2017].

[37] RBS. Cvssv3: New system, next problem (scope). https://www.riskbasedsecurity.com/2017/02/cvssv3-new-system-next-problem-scope/, Fevereiro 2017. [Consult. 10 Set. 2017].

[38] RBS. Cvssv3: New system, old problems remain. https://www.riskbasedsecurity.com/2017/02/cvssv3-new-system-old-problems-remain/, Fevereiro 2017. [Consult. 10 Set. 2017].

[39] RBS. Cvssv3: When every vulnerability appears to be high priority. https://www.riskbasedsecurity.com/2017/05/cvssv3-when-every-vulnerability-appears-to-be-high-priority/, Maio 2017. [Consult. 10 Set. 2017].

[40] Symantec Security Response. What you need to know about the wannacry ransomware. https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware, Maio 2017. [Consult. 20 Set. 2017].

[41] RGPD. Jornal oficial da união europeia. https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf, Maio 2016. [Consult. 11 Maio. 2018].

[42] M. Schiffman. A complete guide to the common vulnerability scoring system (cvss) v1 archive. https://www.first.org/cvss/v1/guide, Junho 2005. [Consult. 2 Jan. 2016].

[43] K. Selvaraj, E. Florio, A. Lelli, T. Ganacharya, and Microsoft Malware Protection Center. Wannacrypt ransomware worm targets out-of-date systems. https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/, Maio 2017. [Consult. 10 Dec. 2017].

[44] S. Spain. New version of common vulnerability scoring system released. https://www.first.org/cvss/v2/, Junho 2017. [Consult. 10 Set. 2017].

[45] G. Spanos and L. Angelis. Impact metrics of securtiy vulnerabilities: Analysis and weighing. *Information Security Journal: A Global Perspective*, 24(1-3):57–71, 2015.

[46] G. Spanos, A. Sioziou, and L. Angelis. Wivss: A new methodology for scoring information systems vulnerabilities. *In Proceedings of the 17th Panhellenic Conference on Informatics (PCI 13)*, pages 83–90, Setembro 2013.

[47] Y. Wang and Y. Yang. Pvl: A novel metric for single vulnerability rating and its application in ims. *Journal of Computational Information Systems*, 8(2):579–590, 2012.

Apêndice A

Avaliação das vulnerabilidades

A.1 NVD

A.1.1 Classificação crítica

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-18001	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17992	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2014-9515	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2014-3630	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Alto	9.5
CVE-2014-0121	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17974	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17968	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2014-4914	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-5641	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8

Tabela A.1 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-17932	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2014-8389	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2015-7669	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2015-6237	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Médio	9.5
CVE-2017-9944	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Médio	9.5
CVE-2017-17931	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17928	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17906	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17900	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17899	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17897	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17895	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17892	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17878	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17877	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17875	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17873	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17872	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17871	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17870	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17849	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-16727	9.1 Crítico	Alto	Alto	Alto	Alto	Nenhum	Nenhum	9.1
CVE-2017-17033	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17032	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17031	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17030	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3

Tabela A.1 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-17029	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17028	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17027	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2015-7224	9.8 Crítico	Alto	Médio	Alto	Alto	Alto	Médio	9.1
CVE-2017-17411	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17821	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Alto	9.1
CVE-2012-2576	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-6094	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2017-16725	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17794	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Médio	9.5
CVE-2017-17790	9.8 Crítico	Alto	Médio	Alto	Alto	Alto	Alto	9.5
CVE-2017-17781	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17779	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17777	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17761	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17759	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17107	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17106	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17105	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-16949	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-15877	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-15875	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-15524	9.1 Crítico	Alto	Alto	Alto	Alto	Nenhum	Nenhum	9.1
CVE-2017-17721	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17651	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17645	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8

Tabela A.1 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-17643	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17739	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17735	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17734	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17733	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17731	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17730	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17717	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2017-17713	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-3195	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-3192	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2017-3191	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2017-3186	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-3185	9.8 Crítico	Alto	Alto	Alto	Médio	Alto	Médio	9.1
CVE-2017-3184	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-14090	9.1 Crítico	Alto	Alto	Alto	Médio	Nenhum	Nenhum	8.4
CVE-2017-10904	9.8 Crítico	Alto	Médio	Alto	Médio	Alto	Médio	8.3
CVE-2017-17701	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17700	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17699	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-14101	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17672	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17671	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17648	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-14590	9.1 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.1
CVE-2017-14589	9.6 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.6

Tabela A.1 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-17642	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17641	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17640	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17639	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17638	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17637	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17636	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17635	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17634	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17633	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17632	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17631	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8
CVE-2017-17630	9.8 Crítico	Alto	Alto	Alto	Alto	Alto	Alto	9.8

Tabela A.1: Avaliação das vulnerabilidades classificação crítica - NVD

A.1.2 Classificação alta

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-17845	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	7,3
CVE-2017-16717	8.6 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	7,8
CVE-2017-14362	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Muito-Baixo	6,6
CVE-2017-2895	8.2 Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	Alto	Alto	7,6

Tabela A.2 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2014-0691	7.3 Alto	Baixo	Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	5,7
CVE-2017-6145	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Muito-Baixo	6,6
CVE-2017-10408	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10407	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10401	8.7 Alto	Baixo	Muito-Baixo	Alto	Alto	Alto	Alto	8,5
CVE-2017-10392	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10391	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,7
CVE-2017-10362	7.2 Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	Baixo	Baixo	6,1
CVE-2017-10360	8.2 Alto	Baixo	Muito-Baixo	Alto	Alto	Nenhum	Nenhum	7,6
CVE-2017-10333	7.4 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,5
CVE-2017-10309	7.1 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,2
CVE-2017-10265	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,7
CVE-2017-10065	8.5 Alto	Baixo	Muito-Baixo	Alto	Alto	Nenhum	Nenhum	7,9
CVE-2017-15575	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	4,7
CVE-2017-1000106	8.5 Alto	Baixo	Muito-Baixo	Alto	Alto	Nenhum	Nenhum	7,9
CVE-2017-1541	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	4,7
CVE-2017-1483	8.6 Alto	Baixo	Baixo	Baixo	Muito-Baixo	Alto	Alto	7,8
CVE-2017-9956	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	4,7
CVE-2015-5184	7.3 Alto	Baixo	Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	5,7
CVE-2016-5795	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	7,3
CVE-2017-12069	8.2 Alto	Baixo	Baixo	Nenhum	Nenhum	Alto	Alto	8,2
CVE-2017-3752	8.2 Alto	Baixo	Muito-Baixo	Alto	Alto	Alto	Alto	8,1
CVE-2017-10242	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10241	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10240	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10239	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2

Tabela A.2 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-10238	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10237	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10236	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10210	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Alto	Alto	6,2
CVE-2017-10278	7.0 Alto	Alto	Alto	Baixo	Muito-Baixo	Baixo	Baixo	6,6
CVE-2017-3446	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-3445	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-3444	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10417	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10416	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10415	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10414	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10413	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10412	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10411	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10410	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10409	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10363	7.1 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	6,6
CVE-2017-10354	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10338	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10326	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10325	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10323	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10312	7.1 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	6,6
CVE-2017-10303	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10263	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6

Tabela A.2 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-10060	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10050	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10034	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10026	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-9625	8.2 Alto	Alto	Alto	Baixo	Baixo	Nenhum	Nenhum	8,2
CVE-2017-11780	7.0 Alto	Alto	Alto	Baixo	Baixo	Baixo	Baixo	7
CVE-2015-7842	7.1 Alto	Nenhum	Nenhum	Baixo	Baixo	Alto	Alto	7,1
CVE-2017-10246	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-10233	7.3 Alto	Nenhum	Nenhum	Baixo	Muito-Baixo	Alto	Alto	7,3
CVE-2017-10226	7.1 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	6,6
CVE-2017-10214	8.2 Alto	Alto	Alto	Baixo	Muito-Baixo	Nenhum	Nenhum	7,6
CVE-2017-15309	7.1 Alto	Nenhum	Nenhum	Alto	Alto	Baixo	Baixo	7,1
CVE-2017-3588	7.3 Alto	Alto	Alto	Alto	Alto	Baixo	Baixo	7,3
CVE-2017-10353	7.1 Alto	Alto	Alto	Nenhum	Nenhum	Baixo	Baixo	7,1
CVE-2017-1192	8.2 Alto	Alto	Alto	Nenhum	Nenhum	Baixo	Baixo	8,2
CVE-2017-10232	7.6 Alto	Alto	Alto	Baixo	Muito-Baixo	Baixo	Baixo	7,2
CVE-2017-10225	7.0 Alto	Alto	Alto	Alto	Alto	Baixo	Baixo	7
CVE-2017-10146	8.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	6,3
CVE-2017-10145	7.4 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,5
CVE-2017-10104	7.4 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,5
CVE-2017-10061	8.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	6,3
CVE-2017-9639	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	7,3
CVE-2017-1254	7.1 Alto	Alto	Alto	Nenhum	Nenhum	Baixo	Baixo	7,1
CVE-2017-6038	7.1 Alto	Nenhum	Nenhum	Baixo	Baixo	Baixo	Muito-Baixo	6,6
CVE-2017-1322	8.2 Alto	Alto	Alto	Nenhum	Nenhum	Baixo	Muito-Baixo	7,6
CVE-2017-6324	7.3 Alto	Baixo	Muito-Baixo	Baixo	Baixo	Baixo	Baixo	6,6

Tabela A.2 continuação da página anterior

Vuln ID	Severidade (CVSS)	Impacto na confidencialidade	Impacto na confidencialidade - Reavaliação	Impacto na integridade	Impacto na integridade - Reavaliação	Impacto na disponibilidade	Impacto na disponibilidade - Reavaliação	Classificação Reavaliada
CVE-2017-7922	7.6 Alto	Alto	Alto	Baixo	Baixo	Baixo	Muito-Baixo	7,2
CVE-2014-0097	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Muito-Baixo	6,6
CVE-2017-8914	8.3 Alto	Baixo	Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	7,4
CVE-2017-1289	8.2 Alto	Alto	Alto	Nenhum	Nenhum	Baixo	Baixo	8,2
CVE-2017-9137	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	7,3
CVE-2017-0279	7.0 Alto	Alto	Alto	Baixo	Baixo	Baixo	Baixo	7
CVE-2017-0278	7.0 Alto	Alto	Alto	Baixo	Baixo	Baixo	Baixo	7
CVE-2017-0277	7.0 Alto	Alto	Alto	Baixo	Baixo	Baixo	Baixo	7
CVE-2017-0249	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	7,3
CVE-2017-7927	7.3 Alto	Baixo	Baixo	Baixo	Baixo	Baixo	Baixo	7,3
CVE-2016-9691	8.6 Alto	Alto	Alto	Baixo	Muito-Baixo	Baixo	Baixo	8,2
CVE-2017-2101	7.3 Alto	Baixo	Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	5,7
CVE-2017-3162	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Muito-Baixo	4,7
CVE-2017-3596	7.6 Alto	Alto	Alto	Baixo	Muito-Baixo	Baixo	Baixo	7,2
CVE-2017-3543	8.6 Alto	Alto	Alto	Baixo	Muito-Baixo	Baixo	Baixo	8,2
CVE-2017-3542	8.6 Alto	Alto	Alto	Baixo	Muito-Baixo	Baixo	Baixo	8,2
CVE-2017-3531	7.2 Alto	Nenhum	Nenhum	Baixo	Muito-Baixo	Baixo	Baixo	6,1
CVE-2017-3507	7.3 Alto	Baixo	Muito-Baixo	Baixo	Muito-Baixo	Baixo	Baixo	5,7

Tabela A.2: Avaliação das vulnerabilidades classificação alta - NVD

A.2 Grupo EDP

A.2.1 Classificação crítica

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
91	A4	Insecure Direct Object References	Alterando o número da conta e o número de contrato, é possível obter dados de outros clientes.	high	Diamond
93	A27	SQL injection	O formulário de esclarecimento de dúvidas encontra-se vulnerável a SQLi	high	Bronze
100	A64	Information Leakage	SAP Management Console - Exposição de Informação Interna	high	Diamond
102	A43	Insufficient Access Control	SQL injection em múltiplos formulários	critical	Bronze
104	A27	SQL injection	SQL injection em múltiplos formulários	critical	Bronze
106	A53	SQL injection	SQL Injection na aplicação A53	high	Gold
121	A43	SQL injection	Acesso a todos os dados da base de dados Oracle	critical	Diamond
123	A79	Insecure Cryptographic Storage	Passwords guardadas em claro na base de dados da aplicação A79	high	Diamond
129	A24	Security Misconfiguration	Credencial por omissão na aplicação A24	high	Diamond
130	A24	Security Misconfiguration	Acesso a informação detalhada sobre as contas de utilizadores da rede interna da EDP	high	Diamond
135	A27	Cross Site Scripting (XSS)	XSS em A27	high	Bronze
140	A73	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A73	high	Bronze
141	A79	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A79	medium	Diamond
144	A79	Cross Site Scripting (XSS)	A aplicação A79 encontra-se vulnerável a Cross-Site Scripting	medium	Diamond
146	A34	Insecure Direct Object References	Acesso a todos os recursos da aplicação sem ser necessário estar autenticado	critical	Silver
147	A17	Security Misconfiguration	Credenciais por omissão com permissões de administração	critical	Gold
152	A17	Using Known Vulnerable Components	Várias vulnerabilidades no IBM Maximo 6.2	critical	Silver
174	A78	Broken Authentication and Session Management	Brute-force na componente de login da aplicação A78	high	Bronze
182	A87	Broken Authentication and	Acesso de administração na aplicação web presente em A87	critical	Bronze

Tabela A.3 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
		Session Management			
185	A33	Cross Site Scripting (XSS)	Stored XSS no parâmetro nickname na aplicação A33	medium	Diamond
186	A33	Cross Site Scripting (XSS)	Stored XSS no parâmetro telemóvel na aplicação A33	medium	Diamond
187	A33	Cross Site Scripting (XSS)	Stored XSS no parâmetro email na aplicação A33	medium	Diamond
191	A87	Unrestricted File Upload	É possível efectuar o upload de qualquer tipo de ficheiro	critical	Bronze
192	A87	Insecure Cryptographic Storage	Credenciais guardadas em claro em ficheiros de configuração	high	Bronze
193	A87	Security Misconfiguration	Execução de comandos de sistema no servidor de base de dados	high	Bronze
194	A87	SQL injection	Injecção de código SQL no parâmetro login	critical	Bronze
195	A12	Cross Site Scripting (XSS)	Stored XSS no parâmetro nome na aplicação A12	medium	Diamond
212	A32	SQL injection	Injecção de código SQL no parâmetro txtDPC	high	Diamond
214	A15	SQL injection	Injecção de código SQL na página de Login	critical	Silver
215	A15	Insufficient Transport Layer Protection	Inexistência de SSL no login e acesso a aplicação web	critical	Silver
327	A66	SQL injection	SQL injection na aplicação A66	high	Gold
328	A66	Weak Password Requirements	Palavra passe fraca	critical	Gold
343	A72	Misconfiguration	Credenciais por omissão na maioria dos dispositivos de A72	high	Bronze
351	A6	Cross Site Scripting (XSS)	Cross Site Scripting em múltiplas páginas	high	Bronze
353	A6	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A6	high	Bronze
355	A6	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A6	high	Bronze
356	A7	Cross Site Scripting (XSS)	Cross Site Scripting em todas as páginas	high	Bronze
374	A8	SQL injection	SQL Injection na aplicação A8	critical	Bronze
377	A8	Weak Credentials	Credenciais de administração fracas	high	Bronze
382	A8	SQL injection	SQL Injection (SQLi) em várias páginas	critical	Bronze
400	A74	Cross Site Scripting (XSS)	Cross Site Scripting em múltiplas páginas	high	Bronze
404	A80	Unrestricted File Upload	Unrestricted File Upload na aplicação A80	critical	Bronze
405	A80	Weak Credentials	Credenciais fracas	critical	Bronze
437	A78	Insecure Direct Object References	Acesso directo a páginas de administração	medium	Bronze
450	A95	Unrestricted File Upload	Unrestricted File Upload na aplicação A95	critical	Bronze

Tabela A.3 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
451	A95	Insecure Direct Object References	Acesso directo a páginas de administração	medium	Bronze
453	A95	Weak Password Requirements	Password guardada em claro na base de dados	critical	Bronze
456	A92	Weak Password Requirements	Password fraca	critical	Silver
458	A92	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A92	medium	Silver
459	A92	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A92	medium	Silver
460	A92	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A92	medium	Silver
463	A10	Cross Site Scripting (XSS)	Cross Site Scripting na página A10	high	Gold
496	A65	Information leakage	Divulgação de cookies de sessão	critical	Bronze
500	A65	Security Misconfiguration	Ausência de credenciais para funcionalidade de deploy	critical	Bronze
510	A90	Cross Site Scripting (XSS)	Cross-site Scripting no parametro lg	high	Bronze
513	A90	Cross Site Scripting (XSS)	Cross-site Scripting - index.asp no parâmetro usuario	high	Bronze
517	A90	Unrestricted File Upload	Possibilidade de upload de ficheiros sem restrições	critical	Bronze
518	A90	Insecure Cryptographic Storage	Ficheiro com pasword de admin gravada em claro	critical	Bronze
539	A22	Broken Authentication and Session Management	Password de administração fraca Password de administração fraca	critical	Bronze
555	A80	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A80	medium	Bronze
560	A41	Broken Authentication and Session Management	Backoffice sem autenticação	medium	Bronze
567	A18	Cross Site Flashing	Cross Site Flashing na aplicação A18	high	Gold
589	A82	Information leakage	Credenciais do WebORB PHP	critical	Bronze
592	A83	Cross Site Scripting (XSS)	Cross Site Scripting na raiz da aplicação	high	Bronze
593	A83	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A83	high	Bronze
594	A83	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A83	high	Bronze
800	A60	Insufficient Access Control	Inexistência de segmentação	critical	Diamond
804	A44	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A44	high	Bronze
808	A44	Cross Site Scripting (XSS)	Cross Site Scripting na aplicação A44	high	Bronze
848	A89	Weak Credentials	Credenciais fracas	critical	Bronze

Tabela A.3 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
867	A81	Unrestricted File Upload	Unrestricted File Upload na aplicação A81	critical	Bronze
868	A65	Security Misconfiguration	Credenciais de origem no acesso à consola de administração do JBoss	critical	Bronze
869	A81	Information leakage	Utilizadores e passwords por omissão no código de backoffice	critical	Bronze
873	A91	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A91	high	Bronze
874	A91	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A91	high	Bronze
886	A93	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A93	high	Bronze
887	A93	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A93	high	Bronze
888	A93	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A93	high	Bronze
889	A93	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A93	high	Bronze
890	A93	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) na aplicação A93	high	Bronze
895	A65	Insecure Cryptographic Storage	Passwords gravadas de forma insegura	critical	Bronze
899	A93	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) stored na aplicação A93	high	Bronze
900	A93	Weak Credentials	Credenciais fracas	critical	Bronze
901	A93	Unrestricted File Upload	Upload de ficheiros sem restrições na aplicação A93	critical	Bronze
902	A93	Information leakage	Ficheiros de bases de dados expostos	critical	Bronze
911	A16	Unrestricted File Upload	Upload de ficheiros sem restrições na aplicação A16	critical	Bronze
912	A16	Unrestricted File Upload	Upload de ficheiros sem restrições na aplicação A16	critical	Bronze
913	A16	Unrestricted File Upload	Upload de ficheiros sem restrições na aplicação A16	critical	Bronze
914	A16	Weak Credentials	Credenciais fracas	critical	Bronze
915	A16	Security Misconfiguration	Passwords guardadas em claro na base de dados	critical	Bronze
926	A10	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) reflectido na aplicação A10	high	Gold
927	A94	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) reflectido na aplicação A94	high	Bronze
930	A95	SQL injection	SQL injection em /webservice.php	critical	Bronze
934	A95	Cross Site Scripting (XSS)	Cross Site Scripting (XSS) persistente na aplicação A95	critical	Bronze
939	A23	Security Misconfiguration	Upload de ficheiros sem restrições	critical	Bronze
945	A95	Weak Credentials	Credenciais fracas	critical	Bronze

Tabela A.3 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
963	A77	SQL injection	SQL injection em A77	critical	Bronze
970	A78	Insufficient Access Control	Configuração do Java RMI vulnerável	critical	Bronze
971	A78	Insecure Cryptographic Storage	Passwords guardadas em claro na base de dados	critical	Bronze
972	A52	Unrestricted File Upload	Carregamento sem restrições de ficheiros	critical	Bronze

Tabela A.3: Sumário das vulnerabilidades na classificação crítica - Grupo EDP

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
463	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1
195	Rede	Baixo	Nenhum	Nenhum	Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1,5
212	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1,5
560	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
804	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
808	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
140	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
400	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
437	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,32	0,04	1	1	0,5
141	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1,5
144	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1,5
555	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
592	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
593	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
594	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
451	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,32	0,04	1	1	0,5
193	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
510	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
513	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
873	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
874	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
458	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1
459	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1
460	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1
886	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
887	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
888	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
889	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
890	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
899	Rede	Baixo	Nenhum	Nenhum	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
377	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
374	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Médio	Médio			
	0,85	0,77	0,85	0,85		0,56	0,32	0,32	1	1	0,5
382	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Médio	Médio			
	0,85	0,77	0,85	0,85		0,56	0,32	0,32	1	1	0,5
214	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Alto	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,32	0,04	1	1	1
147	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Médio
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1
539	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
146	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1
500	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
589	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
182	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
191	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
194	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
517	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
518	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
450	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
453	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
152	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Médio

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,56			
						Médio	Médio	Médio			
	0,85	0,77	0,85	0,85		0,32	0,32	0,32	1	1	1
93	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,32	0,04	1	1	0,5
104	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,32	0,04	1	1	0,5
102	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,32	0,04	1	1	0,5
121	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
215	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Médio
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0,56	0	1	1	1
911	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
912	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
913	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
914	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
915	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
939	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
800	Local	Baixo	Nenhum	Nenhum	Altera	Baixo	Alto	Alto	Não definido	Não definido	Alto
						0,22	0,56	0,56			
						Muito-Baixo	Médio	Alto			
	0,55	0,77	0,85	0,85		0,04	0,32	0,56	1	1	1,5
496	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,32	0,04	1	1	0,5
868	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
895	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
328	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1
970	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
971	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
404	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
405	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
867	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
869	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,32	0,04	1	1	0,5
848	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
456	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,56	0,04	1	1	1
900	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
901	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
902	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
930	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
934	Rede	Baixo	Nenhum	Nenhum	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
945	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
91	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1,5
129	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
130	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
123	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1,5
192	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
351	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
353	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
355	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
356	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
135	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	0,5
100	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Alto	Não definido	Não definido	Alto
						0,56	0	0,56			
						Alto	Nenhum	Médio			
	0,85	0,77	0,85	0,85		0,56	0	0,32	1	1	1,5
187	Rede	Baixo	Baixo	Nenhum	Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,68	0,85		0,56	0,56	0,04	1	1	1,5
926	Rede	Baixo	Nenhum	Requerido	Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,62		0,32	0,32	0,04	1	1	1
327	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Médio	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,32	0,04	1	1	1
343	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
174	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Médio	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,32	0,04	1	1	0,5
972	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,85	0,85		0,56	0,56	0,56	1	1	0,5
963	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	0,5
106	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,56	0,04	1	1	1
185	Rede	Baixo	Baixo	Nenhum	Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto

Tabela A.4 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,68	0,85		0,56	0,56	0,04	1	1	1,5
186	Rede	Baixo	Baixo	Nenhum	Altera	Alto	Alto	Baixo	Não definido	Não definido	Alto
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,68	0,85		0,56	0,56	0,04	1	1	1,5
567	Rede	Baixo	Baixo	Requerido	Altera	Alto	Alto	Alto	Não definido	Não definido	Médio
						0,56	0,56	0,56			
						Alto	Alto	Médio			
	0,85	0,77	0,68	0,62		0,56	0,56	0,32	1	1	1
927	Rede	Baixo	Baixo	Requerido	Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Médio			
	0,85	0,77	0,68	0,62		0,56	0,56	0,32	1	1	0,5

Tabela A.4: Avaliação das vulnerabilidades na classificação crítica - Grupo EDP

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
463	9,6	0,848992	9,6	0,848992
	7,4	0,556096	7,4	0,556096
195	10	0,848992	10	0,870288
	10	0,814144	10	0,818016
212	9,4	0,848992	9,5	0,870288
	9,2	0,814144	9,2	0,818016
560	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
804	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
808	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
140	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
400	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
437	9,4	0,848992	9,3	0,827696
	7,5	0,556096	7,4	0,546848
141	9,6	0,848992	9,6	0,870288
	7,4	0,556096	7,5	0,565344
144	9,6	0,848992	9,6	0,870288
	7,4	0,556096	7,5	0,565344
555	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
592	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
593	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
594	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
451	9,4	0,848992	9,3	0,827696
	7,5	0,556096	7,4	0,546848
193	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
510	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
513	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
873	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
874	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
458	9,6	0,848992	9,6	0,848992
	7,4	0,556096	7,4	0,556096

Tabela A.5 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
459	9,6	0,848992	9,6	0,848992
	7,4	0,556096	7,4	0,556096
460	9,6	0,848992	9,6	0,848992
	7,4	0,556096	7,4	0,556096
886	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
887	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
888	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
889	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
890	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
899	10	0,848992	10	0,827696
	10	0,814144	10	0,810272
377	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
374	9,8	0,914816	9,5	0,860608
	9,1	0,796544	8,7	0,748672
382	9,8	0,914816	9,5	0,860608
	9,1	0,796544	8,7	0,748672
214	9,4	0,848992	9,4	0,848992
	8,5	0,712768	8,5	0,712768
147	9,8	0,914816	9,8	0,914816
	9,8	0,914816	9,8	0,914816
539	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
146	9,4	0,848992	9,4	0,848992
	9,2	0,814144	9,2	0,814144
500	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
589	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
182	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
191	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
194	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
517	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
518	9,4	0,848992	9,3	0,827696

Tabela A.5 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
	9,2	0,814144	9,1	0,810272
450	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
453	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
152	9,8	0,914816	9,8	0,914816
	8,3	0,685568	8,3	0,685568
93	9,4	0,848992	9,3	0,827696
	8,5	0,712768	8,5	0,706784
104	9,4	0,848992	9,3	0,827696
	8,5	0,712768	8,5	0,706784
102	9,4	0,848992	9,3	0,827696
	8,5	0,712768	8,5	0,706784
121	9,8	0,914816	9,8	0,915
	9,8	0,914816	9,8	0,915
215	9,1	0,8064	9,1	0,8064
	9,1	0,8064	9,1	0,8064
911	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
912	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
913	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
914	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
915	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
939	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
800	9,2	0,848992	9,3	0,915
	8,3	0,712768	9,3	0,895552
496	9,4	0,848992	9,3	0,827696
	7,5	0,556096	7,4	0,546848
868	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
895	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
328	9,4	0,848992	9,4	0,848992
	9,2	0,814144	9,2	0,814144
970	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
971	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272

Tabela A.5 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
404	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
405	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
867	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
869	9,4	0,848992	9,3	0,827696
	7,5	0,556096	7,4	0,546848
848	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
456	9,4	0,848992	9,4	0,848992
	8,5	0,712768	8,5	0,712768
900	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
901	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
902	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
930	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
934	10	0,848992	10	0,827696
	10	0,814144	10	0,810272
945	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
91	9,4	0,848992	9,5	0,870288
	9,2	0,814144	9,2	0,818016
129	9,8	0,914816	9,8	0,915
	9,8	0,914816	9,8	0,915
130	9,8	0,914816	9,8	0,915
	9,8	0,914816	9,8	0,915
123	9,4	0,848992	9,5	0,870288
	9,2	0,814144	9,2	0,818016
192	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
351	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
353	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
355	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
356	9,6	0,848992	9,5	0,827696
	7,4	0,556096	7,3	0,546848
135	9,6	0,848992	9,5	0,827696

Tabela A.5 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
	7,4	0,556096	7,3	0,546848
100	9,1	0,8064	9,8	0,915
	8,4	0,7008	8,9	0,7712
187	9,9	0,848992	9,9	0,870288
	9,7	0,814144	9,7	0,818016
926	9,6	0,848992	9,6	0,848992
	7,4	0,556096	7,4	0,556096
327	9,4	0,848992	9,4	0,848992
	7,5	0,556096	7,5	0,556096
343	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
174	9,4	0,848992	9,3	0,827696
	8,5	0,712768	8,5	0,706784
972	9,8	0,914816	9,5	0,860608
	9,8	0,914816	9,5	0,860608
963	9,4	0,848992	9,3	0,827696
	9,2	0,814144	9,1	0,810272
106	9,4	0,848992	9,4	0,848992
	9,2	0,814144	9,2	0,814144
185	9,9	0,848992	9,9	0,870288
	9,7	0,814144	9,7	0,818016
186	9,9	0,848992	9,9	0,870288
	9,7	0,814144	9,7	0,818016
567	9	0,914816	9	0,914816
	9	0,868352	9	0,868352
927	9	0,914816	9	0,860608
	9	0,868352	8,9	0,837376

Tabela A.5: Classificações das vulnerabilidades na classificação crítica - Grupo EDP

A.2.2 Classificação alta

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
122	A79	SQL injection	SQL injection na página de recuperação de password	critical	Diamond
124	A79	Insecure Direct Object References	Acesso a dados pessoais de candidatos	critical	Diamond
158	A79	Misconfiguration	Acesso via telnet sem autenticação ao controlador de acessos WLAN	critical	Bronze
161	A26	Misconfiguration	Acesso com credenciais por omissão	critical	Diamond
172	A61	Using Known Vulnerable Components	Total acesso ao servidor OPC (Gateway) através da exploração da vulnerabilidade MS08-067	critical	Diamond
177	A67	Misconfiguration	Falta de controlo de acesso ao conversor A67	high	Bronze
184	A33	Security Misconfiguration	Acesso a informação dos utilizadores presentes na Active Directory (AD)	high	Diamond
190	A33	Insecure Direct Object References	Detalhes e views do Sharepoint disponíveis a qualquer utilizador registado	medium	Diamond
196	A14	Insecure Direct Object References	Nome e CPE de clientes disponível em A14	medium	Diamond
208	A96	Security Misconfiguration	Enumeração parcial de nomes de ficheiros no servidor IIS	medium	Diamond
218	A15	Broken Authentication and Session Management	Enumeração de utilizadores e revelação de informações	high	Silver
223	A49	Using Known Vulnerable Components	Vulnerabilidade no HP Data Protector acesso a todos os dados	critical	Diamond
224	A48	Using Known Vulnerable Components	Vulnerabilidade no HP Data Protector permite acesso a todos os dados	critical	Diamond
225	A46	Using Known Vulnerable Components	Vulnerabilidade no HP Data Protector permite acesso a todos os dados	critical	Diamond
226	A47	Using Known Vulnerable Components	Vulnerabilidade no SMB permite acesso a todos os dados	critical	Diamond
228	A50	Using Known Vulnerable Components	Vulnerabilidade no DameWare permite acesso	critical	Diamond

Tabela A.6 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
			a todos os dados		
318	A39	Misconfiguration	Acesso de leitura e de escrita via SNMP	high	Bronze
359	A7	SQL injection	SQL injection na página index.php	critical	Bronze
406	A80	Information leakage	Utilizadores/Passwords padrão constantes no código de backoffice	critical	Bronze
412	A10	Broken Authentication and Session Management	Passwords guardadas de forma reversível	high	Gold
438	A98	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A36	high	Bronze
452	A95	Weak Password Requirements	Password guardada em claro num ficheiro de excel	critical	Bronze
473	A88	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
476	A3	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A35	high	Bronze
477	A3	Broken Authentication and Session Management	Acesso directo a páginas de administração	critical	Bronze
478	A3	Weak Password Requirements	Password guardada em claro	critical	Bronze
494	A85	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
508	A90	Broken Authentication and Session Management	Acesso directo a páginas de administração	critical	Bronze
515	A90	Security Misconfiguration	Enumeração parcial de ficheiros e pastas	medium	Bronze
538	A22	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
540	A22	Broken Authentication and Session Management	Privilege escalation	critical	Bronze
542	A22	Insecure Cryptographic Storage	Password guardada em claro num ficheiro de excel	critical	Bronze
557	A80	SQL injection	SQL injection na aplicação A80	high	Bronze
558	A80	SQL injection	SQL injection na aplicação A80	medium	Bronze
563	A41	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
568	A18	Insufficient Transport Layer Protection	Ausência de TLS	high	Gold
576	A20	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
584	A82	Broken Authentication and Session Management	Acesso ao WebORB PHP sem autenticação	critical	Bronze
585	A82	Insecure Direct Object References	Acesso a dados privados sem autenticação	high	Bronze
586	A82	Broken Authentication and Session Management	Acesso a dados pessoais sem autenticação	medium	Bronze
588	A82	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze

Tabela A.6 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
595	A2	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
597	A2	Broken Authentication and Session Management	Ataques de Brute Force possíveis através do xmlrpc.php	medium	Bronze
600	A83	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
602	A2	Broken Authentication and Session Management	Ataques de Brute Force possíveis através do xmlrpc.php	medium	Bronze
609	A84	Security Misconfiguration	Possibilidade de alterar o preço das RECs	critical	Bronze
611	A84	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A37	high	Bronze
615	A5	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze
621	A13	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze
632	A25	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze
634	A29	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze
642	A31	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A31	high	Bronze
648	A35	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A35	high	Bronze
654	A36	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A36	high	Bronze
663	A37	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A37	high	Bronze
664	A38	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A38	high	Bronze
673	A51	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A51	high	Bronze
677	A45	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A45	high	Bronze
684	A54	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A54	high	Bronze
691	A55	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A55	high	Bronze
696	A68	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A68	high	Bronze
703	A69	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A69	high	Bronze
708	A70	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A70	high	Bronze
715	A71	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A71	high	Bronze
722	A75	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A75	high	Bronze
725	A30	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A30	high	Bronze
732	A40	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A40	high	Bronze
738	A21	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze

Tabela A.6 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
744	A62	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A62	high	Bronze
748	A63	Misconfiguration	OpenSSL vulnerável a heartbleed	critical	Bronze
749	A63	Weak Password Requirements	Password fraca	critical	Bronze
758	A99	Denial of Service (DoS)	HTTP.sys vulnerável	critical	Bronze
764	A97	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A38	high	Bronze
769	A19	Weak Credentials	Credenciais de administração fracas	critical	Bronze
778	A59	Using Known Vulnerable Components	Servidor A59 vulneravel a MS08-067	critical	Diamond
779	A56	Using Known Vulnerable Components	Servidor A56 com HP-Dataprotector vulnerável	critical	Diamond
780	A57	Using Known Vulnerable Components	Serviço com SSL vulnerável a HeartBleed	critical	Diamond
789	A42	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
793	A57	Using Known Vulnerable Components	Múltiplas vulnerabilidades	critical	Diamond
794	A59	Using Known Vulnerable Components	Múltiplas vulnerabilidades	critical	Diamond
795	A56	Using Known Vulnerable Components	Múltiplas vulnerabilidades	critical	Diamond
796	A58	Using Known Vulnerable Components	Múltiplas vulnerabilidades	critical	Diamond
803	A44	Insufficient Transport Layer Protection	Ausência de TLS	high	Bronze
815	A52	Security Misconfiguration	Enumeração parcial de ficheiros e pastas	medium	Bronze
821	A28	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze
830	A1	Insufficient Transport Layer Protection	Uso de TLS vulnerável	high	Bronze
836	A76	Insufficient Transport Layer Protection	Uso de TLS vulnerável na aplicação A76	high	Bronze
847	A89	SQL injection	SQL Injection (SQLi) na aplicação A89	critical	Bronze
863	A86	Insufficient Transport Layer Protection	Login com credenciais em claro	high	Silver
885	A80	SQL injection	SQL injection na aplicação A80	critical	Bronze
892	A93	SQL injection	SQL Injection (SQLi) no header de Referer	critical	Bronze
893	A93	SQL injection	SQL Injection (SQLi) na aplicação A93	critical	Bronze
894	A93	SQL injection	SQL Injection (SQLi) na aplicação A93	critical	Bronze
896	A93	SQL injection	SQL Injection (SQLi) na aplicação A93	critical	Bronze
897	A93	SQL injection	SQL Injection (SQLi) na aplicação A93	critical	Bronze

Tabela A.6 continuação da página anterior

Vuln ID	Ativo	Tipo	Sumário	Severidade (Fornecedor)	Criticidade EDP
898	A93	SQL injection	SQL Injection (SQLi) na aplicação A93	critical	Bronze
909	A16	SQL injection	SQL Injection (SQLi) na aplicação A16	critical	Bronze
910	A16	SQL injection	SQL Injection (SQLi) na aplicação A16	critical	Bronze
923	A11	Insecure Direct Object References	Acesso a faturas de outros clientes	critical	Diamond
964	A44	SQL injection	SQL injection na aplicação A44	critical	Bronze

Tabela A.6: Sumário das vulnerabilidades classificação alta - Grupo EDP

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
597	Rede	Baixo	Nenhum	Nenhum	Não altera	Alto	Baixo	Baixo	Não definido	Não definido	Baixo
						0,56	0,22	0,22			
						Médio	Baixo	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,22	0,04	1	1	0,5
602	Rede	Baixo	Nenhum	Nenhum	Não altera	Alto	Baixo	Baixo	Não definido	Não definido	Baixo
						0,56	0,22	0,22			
						Médio	Baixo	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,22	0,04	1	1	0,5
196	Rede	Baixo	Nenhum	Nenhum	Não altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Alto
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	1,5
218	Rede	Baixo	Nenhum	Nenhum	Não altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Médio
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	1
190	Rede	Baixo	Baixo	Nenhum	Não Altera	Alto	Baixo	Baixo	Não definido	Não definido	Alto
						0,56	0,22	0,22			
						Médio	Baixo	Muito-Baixo			
	0,85	0,77	0,68	0,85		0,32	0,22	0,04	1	1	1,5
184	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Alto
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	1,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
557	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
558	Rede	Baixo	Nenhum	Nenhum	Não altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
585	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
586	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
477	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
158	Rede	Baixo	Baixo	Nenhum	Não Altera	Baixo	Alto	Alto	Não definido	Não definido	Baixo
						0,22	0,56	0,56			
						Muito-Baixo	Alto	Alto			
	0,85	0,77	0,62	0,85		0,04	0,56	0,56	1	1	0,5
540	Rede	Baixo	Baixo	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,85	0,77	0,62	0,85		0,56	0,56	0,56	1	1	0,5
542	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
748	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Baixo	Baixo	Não definido	Não definido	Baixo
						0,56	0,22	0,22			
						Médio	Muito-Baixo	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,04	0,04	1	1	0,5
749	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Baixo	Baixo	Não definido	Não definido	Baixo
						0,56	0,22	0,22			
						Alto	Muito-Baixo	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,04	0,04	1	1	0,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
508	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Baixo	Baixo	Não definido	Não definido	Baixo
						0,56	0,22	0,22			
						Alto	Muito-Baixo	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,56	0,04	0,04	1	1	0,5
892	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
893	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
896	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
897	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
898	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
758	Rede	Baixo	Nenhum	Nenhum	Não Altera	Nenhum	Nenhum	Alto	Não definido	Não definido	Baixo
						0	0	0,56			
						Nenhum	Nenhum	Alto			
	0,85	0,77	0,85	0,85		0	0	0,56	1	1	0,5
452	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	0,5
124	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Alto
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	1,5
122	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Alto
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	1,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
478	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
359	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
923	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Alto
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	1,5
909	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
910	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
769	Rede Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Baixo
						0,56	0,56	0,56			
						Médio	Alto	Alto			
	0,62	0,77	0,85	0,85		0,32	0,56	0,56	1	1	0,5
172	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
161	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
225	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
226	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
224	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
223	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
228	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
779	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
795	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
780	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
793	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
796	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
778	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5
794	Local	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Alto	Não definido	Não definido	Alto
						0,56	0,56	0,56			
						Alto	Alto	Alto			
	0,55	0,77	0,85	0,85		0,56	0,56	0,56	1	1	1,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
406	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Baixo	Baixo	Não definido	Não definido	Baixo
						0,56	0,22	0,22			
						Médio	Muito-Baixo	Muito-Baixo			
	0,85	0,77	0,85	0,85		0,32	0,04	0,04	1	1	0,5
885	Rede	Baixo	Nenhum	Nenhum	Não Altera	Nenhum	Alto	Baixo	Não definido	Não definido	Baixo
						0	0,56	0,22			
						Nenhum	Alto	Muito-Baixo			
	0,85	0,77	0,85	0,85		0	0,56	0,04	1	1	0,5
609	Rede	Baixo	Nenhum	Nenhum	Não Altera	Nenhum	Alto	Nenhum	Não definido	Não definido	Baixo
						0	0,56	0			
						Nenhum	Médio	Nenhum			
	0,85	0,77	0,85	0,85		0	0,32	0	1	1	0,5
847	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
894	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Baixo
						0,56	0	0			
						Médio	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,32	0	0	1	1	0,5
830	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
595	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
615	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
621	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
576	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
738	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
538	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
632	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
821	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
634	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
725	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
642	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
648	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
654	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
663	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
664	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
476	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
438	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
611	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
764	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
732	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
563	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
789	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
803	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
677	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
673	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
684	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
691	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
744	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
722	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
836	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
696	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
703	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
708	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
715	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
588	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
600	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
494	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
863	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Médio
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	1
473	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Baixo
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	0,5
318	Rede	Baixo	Nenhum	Nenhum	Não Altera	Baixo	Alto	Nenhum	Não definido	Não definido	Baixo
						0,22	0,56	0			
						Muito-Baixo	Médio	Nenhum			
	0,85	0,77	0,85	0,85		0,04	0,32	0	1	1	0,5
964	Rede	Baixo	Baixo	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Baixo
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,62	0,85		0,56	0,56	0,04	1	1	0,5
412	Rede	Baixo	Baixo	Nenhum	Não Altera	Alto	Alto	Baixo	Não definido	Não definido	Médio
						0,56	0,56	0,22			
						Alto	Alto	Muito-Baixo			
	0,85	0,77	0,62	0,85		0,56	0,56	0,04	1	1	1
815	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Alto	Não definido	Não definido	Baixo
						0,56	0	0,56			
						Alto	Nenhum	Alto			
	0,85	0,77	0,85	0,85		0,56	0	0,56	1	1	0,5
584	Rede	Baixo	Nenhum	Nenhum	Não Altera	Baixo	Alto	Alto	Não definido	Não definido	Baixo
						0,22	0,56	0,56			
						Baixo	Alto	Alto			
	0,85	0,77	0,85	0,85		0,22	0,56	0,56	1	1	0,5

Tabela A.7 continuação da página anterior

Vuln ID	Superficie de ataque	Complexidade do ataque	Privilégios requeridos	Interação do utilizador	Âmbito	Confidencialidade	Integridade	Disponibilidade	Requisitos na Confidencialidade	Requisitos na Integridade	Requisitos na Disponibilidade
177	Rede	Baixo	Nenhum	Nenhum	Não Altera	Baixo	Alto	Alto	Não definido	Não definido	Baixo
						0,22	0,56	0,56			
						Muito-Baixo	Alto	Alto			
	0,85	0,77	0,85	0,85		0,04	0,56	0,56	1	1	0,5
568	Adjacente	Baixo	Nenhum	Nenhum	Não Altera	Alto	Alto	Nenhum	Não definido	Não definido	Médio
						0,56	0,56	0			
						Alto	Alto	Nenhum			
	0,62	0,77	0,85	0,85		0,56	0,56	0	1	1	1
515	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Alto	Não definido	Não definido	Baixo
						0,56	0	0,56			
						Alto	Nenhum	Alto			
	0,85	0,77	0,85	0,85		0,56	0	0,56	1	1	0,5
208	Rede	Baixo	Nenhum	Nenhum	Não Altera	Alto	Nenhum	Nenhum	Não definido	Não definido	Alto
						0,56	0	0			
						Alto	Nenhum	Nenhum			
	0,85	0,77	0,85	0,85		0,56	0	0	1	1	1,5

Tabela A.7: Avaliação das vulnerabilidades na classificação alta - Grupo EDP

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
597	8,6	0,732304	8,4	0,694552
	7,1	0,490816	7	0,480208
602	8,6	0,732304	8,4	0,694552
	7,1	0,490816	7	0,480208
196	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
218	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
190	7,9	0,732304	8,1	0,770056
	6,3	0,490816	6,4	0,501424
184	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
557	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
558	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
585	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
586	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
477	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
158	8,3	0,848992	7,7	0,752896
	8,1	0,814144	7,4	0,695872
540	8,8	0,914816	8,4	0,860608
	8,8	0,914816	8,4	0,860608
542	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
748	8,6	0,732304	8,4	0,694552
	6,3	0,373312	6,2	0,360256
749	8,6	0,732304	8,4	0,694552
	7,8	0,594496	7,7	0,586048
508	8,6	0,732304	8,4	0,694552
	7,8	0,594496	7,7	0,586048
892	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
893	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
896	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
897	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
898	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56

Tabela A.8 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
758	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
452	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
124	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
122	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
478	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
359	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
923	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56
909	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
910	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
769	8,8	0,914816	8,4	0,860608
	8,5	0,868352	7,9	0,784576
172	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
161	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
225	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
226	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
224	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
223	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
228	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
779	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
795	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
780	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
793	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
796	8,4	0,914816	8,4	0,915

Tabela A.8 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
	8,4	0,914816	8,4	0,915
778	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
794	8,4	0,914816	8,4	0,915
	8,4	0,914816	8,4	0,915
406	8,6	0,732304	8,4	0,694552
	6,3	0,373312	6,2	0,360256
885	8,2	0,6568	7,8	0,6084
	7,6	0,5776	7,6	0,5688
609	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
847	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
894	7,5	0,56	7,5	0,56
	6	0,32	6	0,32
830	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
595	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
615	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
621	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
576	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
738	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
538	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
632	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
821	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
634	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
725	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
642	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
648	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
654	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064

Tabela A.8 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
663	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
664	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
476	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
438	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
611	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
764	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
732	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
563	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
789	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
803	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
677	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
673	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
684	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
691	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
744	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
722	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
836	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
696	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
703	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
708	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
715	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
588	8,1	0,8064	8,1	0,8064

Tabela A.8 continuação da página anterior

Vuln ID	Classificação MB	ISC Base	Classificação MA	ISC Alterado
	8,1	0,8064	8,1	0,8064
600	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
494	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
863	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
473	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
318	8,2	0,6568	8,2	0,6568
	6,2	0,3472	6,2	0,3472
964	8,3	0,848992	8,2	0,827696
	8,1	0,814144	8,1	0,810272
412	8,3	0,848992	8,3	0,848992
	8,1	0,814144	8,1	0,814144
815	9,1	0,8064	8,3	0,6832
	9,1	0,8064	8,3	0,6832
584	9,4	0,848992	8,8	0,752896
	9,4	0,848992	8,8	0,752896
177	9,4	0,848992	8,8	0,752896
	9,2	0,814144	8,4	0,695872
568	8,1	0,8064	8,1	0,8064
	8,1	0,8064	8,1	0,8064
515	9,1	0,8064	8,3	0,6832
	9,1	0,8064	8,3	0,6832
208	7,5	0,56	7,5	0,56
	7,5	0,56	7,5	0,56

Tabela A.8: Classificações das vulnerabilidades na classificação alta - Grupo EDP