

SEGURANÇA DE SISTEMAS INFORMÁTICOS

Ficha 1 - Vulnerabilidades e Exposições Comuns (CVE)

Maria Miguel Regueiras A85242

Mestrado Integrado em Engenharia Informática

Universidade do Minho

27 de outubro de 2020

Conteúdo

1	Exercício 1	2
2	Exercício 2	6
3	Exercício 3	10
4	Exercício 4	11

Lista de Figuras

1	Vulnerabilidade CVE-2020-6842	2
2	Vulnerabilidade CVE-2018-1167	3
3	Descrição do vetor da vulnerabilidade	3
4	Pesquisa no Exploit-DB	4
5	Vulnerabilidade CVE-2020-15140	4
6	Vulnerabilidade CVE-2020-12401	5
7	Relatório da Mozilla	5
8	Explicação do Heartbleed	7
9	Vulnerabilidade CVE-2014-0160	7
10	Vetor segundo a versão 2.0	8
11	Vetor segundo a versão 3.1	8
12	Explicação do exploit do CVE-2014-0160	9
13	Impacto da vulnerabilidade CVE-2014-0160	9
14	Vulnerabilidade CVE-2020-15670	10
15	Vulnerabilidade CVE-2020-15671	10
16	Vulnerabilidade CVE-2020-15664	11
17	CWE-346: Origin Validation Error	12
18	CWE-348: Use of Less Trusted Source	12

1 Exercício 1

Q: Escolha três aplicações tipicamente usadas em seu computador pessoal, pesquise pela existência de vulnerabilidades conhecidas e meios de explorá-las. Descreva detalhadamente as suas descobertas, incluindo as imagens de suas pesquisas e a descrição das informações nelas contidas.

R: As três aplicações escolhidas foram "Spotify", "Discord" e "Firefox", e para a pesquisa das suas vulnerabilidades foram usados vários sites como NVD e CVE. Para exploração dos seus possíveis exploits foi usado o site Exploit-DB.

Spotify

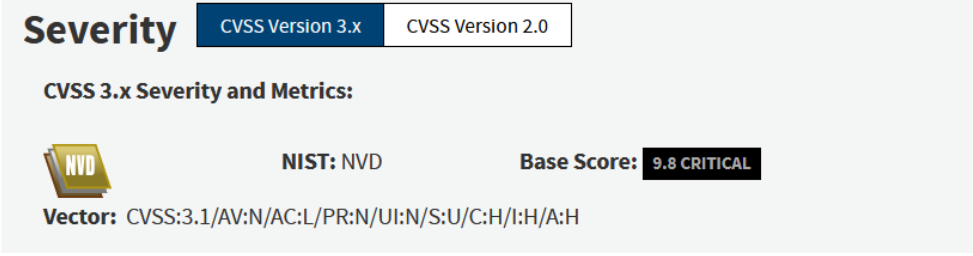
- NVD

CVE-2020-6841 Detail

Current Description

D-Link DCH-M225 1.05b01 and earlier devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the spotifyConnect.php userName parameter.

[+View Analysis Description](#)



The screenshot displays the NVD entry for CVE-2020-6841. It features a 'Severity' section with tabs for 'CVSS Version 3.x' and 'CVSS Version 2.0'. Below this, the 'CVSS 3.x Severity and Metrics' are shown, including a 'NIST: NVD' label, a 'Base Score: 9.8 CRITICAL' badge, and a 'Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H'.


Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
	NIST: NVD	Base Score: 9.8 CRITICAL
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Figura 1: Vulnerabilidade CVE-2020-6842

De acordo com a descrição da vulnerabilidade ("Current Discription") podemos saber os detalhes desta e qual a sua possível exploração. Neste caso, indica-nos que possíveis atacantes podem executar comandos via shell do sistema operativo remotamente. Para além disso, a sua classificação ("Base Score") da sua gravidade é de 9.8 significando que é uma vulnerabilidade crítica ou muito perigosa.

Segundo o NVD, existe um exploit conhecido desta vulnerabilidade que se encontra neste [link](#).

- CVE

CVE-ID	
CVE-2018-1167	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Spotify Music Player 1.0.69.336. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of URI handlers. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5501.	

Figura 2: Vulnerabilidade CVE-2018-1167

Segundo o CVE, a última vulnerabilidade reportada foi a que se pode observar na imagem. Tal como a anterior, podemos ler a sua descrição detalhada. Neste caso, esta vulnerabilidade permitia que possíveis atacantes pudessem executar código em instalações mais vulneráveis da aplicação na versão 1.0.69.336. Neste caso seria necessário o utilizador abrir uma página ou ficheiro malicioso.

CVSS v3.0 Severity and Metrics:	
Base Score:	8.8 HIGH
Vector:	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Impact Score:	5.9
Exploitability Score:	2.8
<hr/>	
Attack Vector (AV):	Network
Attack Complexity (AC):	Low
Privileges Required (PR):	None
User Interaction (UI):	Required
Scope (S):	Unchanged
Confidentiality (C):	High
Integrity (I):	High
Availability (A):	High

Figura 3: Descrição do vetor da vulnerabilidade

Procurando no NVD pela gravidade da vulnerabilidade, esta tinha uma classificação de 8.8 (alta) e na descrição do vetor podemos observar que é necessário de facto a interação do utilizador.

A procura de um exploit no site Exploit-DB não teve sucesso e não se encontrou a publicação de um possível exploit para esta vulnerabilidade.

☐ Verified
 ☐ Has App

Filters
 Reset All

Show 15

Search: CVE-2018-1167

Date D A V Title
 Type Platform Author

No matching records found

Showing 0 to 0 of 0 entries (filtered from 43,163 total entries)
 FIRST
 PREVIOUS
 NEXT
 LAST

Figura 4: Pesquisa no Exploit-DB

Discord

- NVD

CVE-2020-15140 Detail

Current Description

In Red Discord Bot before version 3.3.11, a RCE exploit has been discovered in the Trivia module: this exploit allows Discord users with specifically crafted usernames to inject code into the Trivia module's leaderboard command. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. This critical exploit has been fixed on version 3.3.11.


[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0


CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 9.6 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N



CNA: GitHub, Inc.

Base Score: 8.2 HIGH

Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N

Figura 5: Vulnerabilidade CVE-2020-15140

Segundo a descrição da vulnerabilidade, esta é relacionada com um bot que é possível ter na aplicação. Com usernames específicos, era possível injetar código num dos módulos e realizar ações destrutivas e aceder a informação do utilizador. Diz ainda que a sua gravidade é de 9.6 (crítica) e foi corrigida na versão 3.3.11.

No entanto, não se encontrou nenhum exploit publicado.

Firefox

- NVD

CVE-2020-12401 Detail

UNDERGOING ANALYSIS

This vulnerability is currently undergoing analysis and not all information is available. Please check back soon to view the completed vulnerability summary.

Description


During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data. This vulnerability affects Firefox < 80 and Firefox for Android < 80.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:

**NIST: NVD**

Base Score: N/A

NVD score not yet provided.

Figura 6: Vulnerabilidade CVE-2020-12401

Neste caso, a vulnerabilidade é tão recente (relativamente à data em que este relatório foi escrito) que não existe sequer uma avaliação da sua gravidade. Como podemos observar, no topo a laranja lê-se que ainda está sob análise.

CVE-2020-12401: Timing-attack on ECDSA signature generation

Reporter Sohaib ul Hassan, Iaroslav Gridin, Ignacio M. Delgado-Lozano, Cesar Pereida García, Jesús-Javier Chi-Domínguez, Alejandro Cabrera Aldaya, and Billy Bob Brumley, Network and Information Security (NISEC) Group, Tampere University, Finland

Impact moderate

Description

During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data.

References

[Bug 1631573](#)

Figura 7: Relatório da Mozilla

Após a procura de exploits possíveis (sem sucesso) uma pesquisa no Google levou ao relatório da própria Mozilla onde podemos ler o impacto que teve (moderado).

2 Exercício 2

Q: Em 2014 foi descoberta uma falha de programação na biblioteca de criptografia open source OpenSSL que ficou publicamente conhecida como Heartbleed. Esta falha foi identificada com CVE-2014-0160. Use esta identificação para descrever detalhadamente esta falha, incluindo (mas não apenas) as versões afetadas, os eventuais exploits existentes, vectores de ataque, impacto e soluções. Use as imagens de suas consultas e outros recursos utilizados para justificar suas conclusões.

R: O bug *Heartbleed* identificado como CVE-2014-0160 é uma vulnerabilidade da biblioteca OpenSSL que permitia a atacantes enviar pacotes que possibilitavam a leitura de dados privados através de uma técnica de buffer over-read. Estas informações lidas incluíam chaves privadas que eram usadas para encriptar tráfego e passwords, permitindo que estes roubassem informações importantes.

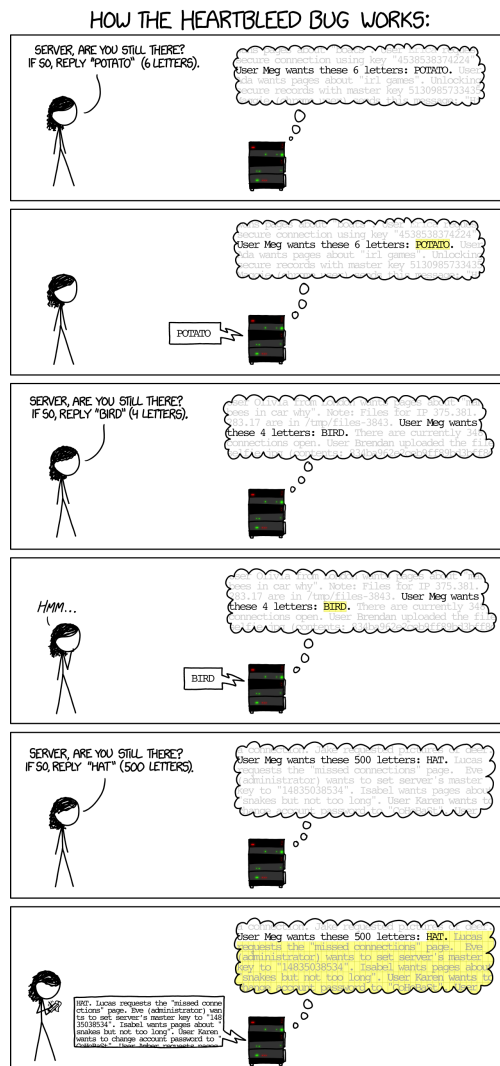


Figura 8: Explicação do Heartbleed

Segundo o NVD:

CVE-2014-0160 Detail

Current Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Figura 9: Vulnerabilidade CVE-2014-0160

E de facto, visto a biblioteca em causa ser open source, qualquer pessoa conseguiria ir verificar em que parte do código estaria o erro que provocava a existência desta vulnerabilidade. E se repararmos, esta resume-se a uma linha de código:

```
memcpy(destino, origem, x);
```

A função `memcpy` copia da variável `origem` `x` bytes para a variável `destino`. Mas em nenhum lado `x` estava a ser verificado, abrindo assim uma oportunidade para atacantes se aventurarem e pedirem tamanhos maiores do que deviam, e obterem informações a mais.

A classificação dos vetores varia bastante da versão 2 para a versão 3.1:

CVSS v2.0 Severity and Metrics:

Base Score: 5.0 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

Access Vector (AV): Network

Access Complexity (AC): Low

Authentication (AU): None

Confidentiality (C): Partial

Integrity (I): None

Availability (A): None

Additional Information:

Allows unauthorized disclosure of information

Figura 10: Vetor segundo a versão 2.0

CVSS v3.1 Severity and Metrics:

Base Score: 7.5 HIGH

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Impact Score: 3.6

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): None

Availability (A): None

Figura 11: Vetor segundo a versão 3.1

Como podemos observar, na versão 2.0, ele apenas está classificado com gravidade 5.0 (médio) quando na realidade é bastante mais alto segundo a versão 3.1, 7.5 (alto). Isto deve-se ao facto de estarem a ser avaliados parâmetros diferentes, levando a uma descrição da realidade não tão precisa. Analisando então a versão 3.1, este vetor utiliza a rede, é de baixa complexidade e não necessita de privilégios nem da intervenção direta do utilizador. Isto torna a que pareça simples explorar esta vulnerabilidade com o exploit certo.

As versões afetadas são todas entre a 1.0.1 e a 1.0.1f. Existem alguns exploits no Exploit-DB visto este bug ser bastante conhecido, um dos possíveis sendo [este](#).

Segundo a explicação deste exploit em particular, este refere que o exploit tira partido do facto de não haver validação do tamanho inserido no pedido, havendo possível acesso à heap do cliente. Este consegue retirar 65532 bytes de informação da heap por cada pedido e pode estar em execução até a conexão ser fechada.


```

/*
 * CVE-2014-0160 heartbleed OpenSSL information leak exploit
 * =====
 * This exploit uses OpenSSL to create an encrypted connection
 * and trigger the heartbleed leak. The leaked information is
 * returned within encrypted SSL packets and is then decrypted
 * and wrote to a file to annoy IDS/forensics. The exploit can
 * set heartbeat payload length arbitrarily or use two preset
 * values for NULL and MAX length. The vulnerability occurs due
 * to bounds checking not being performed on a heap value which
 * is user supplied and returned to the user as part of DTLS/TLS
 * heartbeat SSL extension. All versions of OpenSSL 1.0.1 to
 * 1.0.1f are known affected. You must run this against a target
 * which is linked to a vulnerable OpenSSL library using DTLS/TLS.
 * This exploit leaks upto 65532 bytes of remote heap each request
 * and can be run in a loop until the connected peer ends connection.
 * The data leaked contains 16 bytes of random padding at the end.
 * The exploit can be used against a connecting client or server,
 * it can also send pre_cmd's to plain-text services to establish
 * an SSL session such as with STARTTLS on SMTP/IMAP/POP3. Clients
 * will often forcefully close the connection during large leak
 * requests so try to lower your payload request size.
 *

```

Figura 12: Explicação do exploit do CVE-2014-0160

O impacto desta vulnerabilidade e posterior exploração também está descrita juntamente com os detalhes desta. Como podemos observar na imagem seguinte, é dito que o impacto depende do tipo de informação que pode ser furtada. Faz sentido que tenha mais impacto se a informação seja mais importante (como chaves e passwords) e menos impacto caso contrário.

Após a vulnerabilidade ter sido publicada, várias empresas tentaram corrigir o erro atempadamente, mas ainda assim houve estragos. Por exemplo, várias informações foram roubadas relativamente a pacientes e os seus respetivos dados.

Evaluator Impact

CVSS V2 scoring evaluates the impact of the vulnerability on the host where the vulnerability is located. When evaluating the impact of this vulnerability to your organization, take into account the nature of the data that is being protected and act according to your organization's risk acceptance. While CVE-2014-0160 does not allow unrestricted access to memory on the targeted host, a successful exploit does leak information from memory locations which have the potential to contain particularly sensitive information, e.g., cryptographic keys and passwords. Theft of this information could enable other attacks on the information system, the impact of which would depend on the sensitivity of the data and functions of that system.

Figura 13: Impacto da vulnerabilidade CVE-2014-0160

A solução deste bug passou por passar a verificar-se de o tamanho de leitura pedido era válido certificando-se que não enviava informações na memória contígua ao sítio onde o pedido se encontrasse, uma solução bastante simples.

3 Exercício 3

Q: Assim como diversas corporações, a Mozilla Foundation divulga informações sobre vulnerabilidades as quais os seus produtos foram expostos através do seu Security Advisories. Em 02 de setembro de 2020, a companhia disponibilizou uma atualização do seu browser, i.e., Firefox for Android 80. Esta versão resolve uma série de vulnerabilidades listadas no relatório. Descreva detalhadamente três vulnerabilidades listadas neste relatório.

R: Escolhendo arbitrariamente 3 das vulnerabilidades existentes no relatório da Mozilla, foram selecionadas as seguintes:

CVE-2020-15670: Memory safety bugs fixed in Firefox for Android 80

Reporter Mozilla developers

Impact high

Description

Mozilla developers Jason Kratzer, Christian Holler, and Byron Campen reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

References

[Memory safety bugs fixed in Firefox for Android 80](#)

Figura 14: Vulnerabilidade CVE-2020-15670

Primeiramente, foi reportado um bug que envolvia corrupção de memória que podia ser alvo de ataques e com algum esforço, ser explorada de forma a permitir correr código malicioso. Segundo a Mozilla esta teve um impacto alto e segundo o NVD tem gravidade de 8.8 (alta).

CVE-2020-15671: Passwords could be saved to phone keyboard dictionary

Reporter Karol Frejlich

Impact low

Description

When typing in a password under certain conditions, a race may have occurred where the InputContext was not being correctly set for the input field, resulting in the typed password being saved to the keyboard dictionary.

References

[Bug 1653862](#)

Figura 15: Vulnerabilidade CVE-2020-15671

Seguidamente encontramos uma vulnerabilidade bastante curiosa que se relaciona com as passwords do utilizador. Podia ocorrer que o campo onde o input seria introduzido não estivesse bem direcionado e quando o utilizador introduzisse a sua password, esta fosse guardada no dicionário do teclado. Esta vulnerabilidade foi classificada com um impacto baixo pela Mozilla e a sua gravidade segundo o NVD é de 3.1 (baixa).

CVE-2020-15664: Attacker-induced prompt for extension installation

Reporter Kaizer Soze

Impact high

Description

By holding a reference to the `eval()` function from an `about:blank` window, a malicious webpage could have gained access to the `InstallTrigger` object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed.

References

[Bug 1658214](#)

Figura 16: Vulnerabilidade CVE-2020-15664

Por fim, foi escolhida uma vulnerabilidade com um impacto alto segundo a Mozilla e segundo o NVD com uma gravidade avaliada em 6.5 (média). Esta relaciona-se com a referência de uma função `eval()` de uma janela `about:blank`, onde uma página maliciosa poderia ganhar acesso ao objeto `InstallTrigger` e assim permitir questionar ao utilizador se desejava instalar uma extensão. Refere ainda que o utilizador teria de tomar alguma ação e que, se estivesse confuso, poderia aceitar a instalação e assim instalar algo malicioso.

4 Exercício 4

Q: Recorrendo ao CWE, descreva dois tipos comuns de problemas relacionados com integridade de dados identificados no desenvolvimento de software.

R: Dois tipos comuns de problemas são por exemplo a má validação da origem os dados e o uso de uma fonte de dados menos fiável. Como os próprios nomes indicam, ambas são relacionadas com o local de origem das informações. Na primeira passa por não se verificar se a origem é realmente válida, e a segunda acontece quando por exemplo existem mais do que um local onde se pode ir buscar os dados mas o software escolhe a fonte menos fiável delas. Isto afeta a integridade dos dados pois visto que as fontes podem ser dúbias, também podem ser os próprios dados em questão.

CWE-346: Origin Validation Error

Weakness ID: 346
Abstraction: Base
Structure: Simple

Presentation Filter:

Complete

▼ Description

The software does not properly verify that the source of data or communication is valid.

Figura 17: CWE-346: Origin Validation Error

CWE-348: Use of Less Trusted Source

Weakness ID: 348
Abstraction: Base
Structure: Simple

Presentation Filter:

Complete

▼ Description

The software has two different sources of the same data or information, but it uses the source that has less support for verification, is less trusted, or is less resistant to attack.

Figura 18: CWE-348: Use of Less Trusted Source