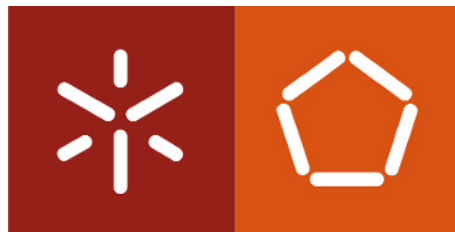


Tecnologia de Segurança

26 de Outubro de 2020

TP1

a83899 André Morais



Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1	Pergunta 1	2
1.1	Google Chrome	2
1.1.1	Exploitability metrics	3
1.1.2	Scope	3
1.1.3	Impact metrics	3
1.2	Spotify	5
1.2.1	Exploitability metrics	5
1.2.2	Scope	6
1.2.3	Impact metrics	6
1.3	Discord	7
1.3.1	Exploitability metrics	8
1.3.2	Scope	8
1.3.3	Impact metrics	8
2	Pergunta 2	9
3	Pergunta 3	11
3.1	Passwords podiam ser guardadas no dicionário do teclado do telemóvel	11
3.2	As Condition Race quando lidas, certificavam a informação . .	12
3.3	Memory safety bugs fixed	13
4	Pergunta 4	14
4.1	Download de Código sem Verificação de Integridade	14
4.2	Confiança nas Cookies sem Validação e Verificação da Integri- dade	14

1 Pergunta 1

1.1 Google Chrome

- **CVE :** CVE-2020-9633
- **Descrição :** Todas as versões do *chrome-launcher* permitem a execução de comandos arbitrários. O *chrome-launcher* é uma biblioteca para iniciar o Google Chrome mais facilmente. Estando esta versão afetada, estão vulneráveis ao comando *Injection*. Controlando o **\$HOME** num operdador Linux, um atacante pode executar código arbitrário
- **Solução:** Atualizar o *chrome-launcher* para a versão 0.13.2 ou acima.
- **NVD Publicado :** 05/02/2020
- **Última Modificação do NVD :** 05/07/2020
- **CVSS Severity Scale :** Critical (9.8)

CVE ID	
CVE-2020-7645 Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information	
Description	
All versions of chrome-launcher allow execution of arbitrary commands, by controlling the \$HOME environment variable in Linux operating systems.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://snky.io/vuln/SNYK-JS-CHROME-LAUNCHER-537575	
Assigning CNA	
Snyk	
Date Entry Created	
20200121	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20200121)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an entry on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the CVE Reference Maps .	
For More Information: CVE Request Web Form (select "Other" from dropdown)	

Figura 1: CVE de vulnerabilidade

1.1.1 Exploitability metrics

- **Attack Vector (AV)** : Network. Significa que a componente vulnerável é marcada para a network stack e o attacker's path é através da camada 3 do OSI (the network layer)
- **Attack Complexity (AC)** : Baixa. Condições de acesso especializadas ou mais complicadas não existem. O atacante tem sucesso contra esta vulnerabilidade
- **Privileges required (PR)** : Nenhum. O atacante não precisa de acesso às definições ou ficheiros para continuar o ataque
- **User Interaction (UI)** : Nenhuma. A vulnerabilidade pode ser explorada sem a intervenção de qualquer utilizador

1.1.2 Scope

- **Scope (S)** : Inalterado. Uma vulnerabilidade explorada apenas pode afetar os recursos geridos pela mesma autoridade. Neste caso a vulnerabilidade da componente e o impacto desta são os mesmos

1.1.3 Impact metrics

- **Confidentiality impact (C)** : Alta. Há uma perda total de confidencialidade, resultando em todos os recursos dentro da componente que sofreu o "impacto" serem divulgados para o atacante
- **Integrity impact (I)** : Alta. Há total perda de integridade ou perda total de proteção
- **Availability impact (A)** : Alta. Não há disponibilidade, no que resulta no atacante ser completamente capaz de negar o acesso aos recursos das componentes atacadas.

CVSS v3.1 Severity and Metrics:

Base Score: 9.8 CRITICAL

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

Impact Score: 5.9

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): High

Availability (A): High

Figura 2: CVSS de vulnerabilidade

1.2 Spotify

- **CVE** : CVE-2018-1167
- **Descrição** : Esta vulnerabilidade permite aos atacantes remotos a executarem código nas instalações vulneráveis do Spotify Music Player 1.0.69.336. É necessária a interação de um User para explorar esta vulnerabilidade com o objetivo de visitar uma página maliciosa ou abrir ficheiros maliciosos. Este problema resulta da falta de validação apropriada.
- **NVD Publicado** : 04/18/2018
- **Última Modificação do NVD** : 10/09/2019
- **Solução**: Resolvida na versão 1.0.73.345
- **CVSS Severity Scale** : **High** (8.8)

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.	
References	
Notes: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC: https://zerodayinitiative.com/advisories/ZDI-18-280	
Assigning CNA	
Zero Day Initiative	
Date Entry Created	
20171205	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20171205)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an entry on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the CVE Reference Maps .	
For More Information: CVE Request Web Form (select "Other" from dropdown)	

Figura 3: CVE de vulnerabilidade

1.2.1 Exploitability metrics

- **Attack Vector (AV)** : Network.
- **Attack Complexity (AC)** : Baixa.
- **Privileges required (PR)** : Nenhuma.
- **User Interaction (UI)** : Necesária.

1.2.2 Scope

- Scope (S) : Inalterado.

1.2.3 Impact metrics

- Confidentiality impact (C) : Alta.
- Integrity impact (I) : Alta.
- Availability impact (A) : Alta.

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

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 4: CVSS de vulnerabilidade

1.3 Discord

- **CVE** : CVE-2020-24928
- **Descrição** : Sem este patch qualquer website podia ter a informação dos users do Discord se a aplicação PreMiD estivesse a correr em back-ground
- **NVD Publicado** : 08/29/2020
- **Última Modificação do NVD** : 09/03/2020
- **CVSS Severity Scale** : **Medium** (5.3)

CVE ID	
CVE-2020-24928 Learn more at National Vulnerability Database (NVD)	
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information	
Description	
managers/socketManagers in PreMiD through 2.1.3 has a locally hosted socketio web server (port 3020) open to all origins, which allows attackers to obtain sensitive Discord user information.	
References	
Note: <i>References</i> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC: https://github.com/PreMiD/PreMiD/pull/501	
Assigning CNA	
MITRE Corporation	
Date Entry Created	
20200828	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20200828)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an entry on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the CVE Reference Maps .	
For More Information: CVE Request Web Form (select "Other" from dropdown)	

Figura 5: CVE de vulnerabilidade

1.3.1 Exploitability metrics

- **Attack Vector (AV)** : Network.
- **Attack Complexity (AC)** : Baixa.
- **Privileges required (PR)** : Nenhuma.
- **User Interaction (UI)** : Nenhuma.

1.3.2 Scope

- **Scope (S)** : Inalterado

1.3.3 Impact metrics

- **Confidentiality impact (C)** : Baixa.
- **Integrity impact (I)** : Nenhuma.
- **Availability impact (A)** : Nenhuma.

CVSS v3.1 Severity and Metrics:

Base Score: 5.3 MEDIUM

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

Impact Score: 1.4

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): Low

Integrity (I): None

Availability (A): None

Figura 6: CVSS de vulnerabilidade

2 Pergunta 2

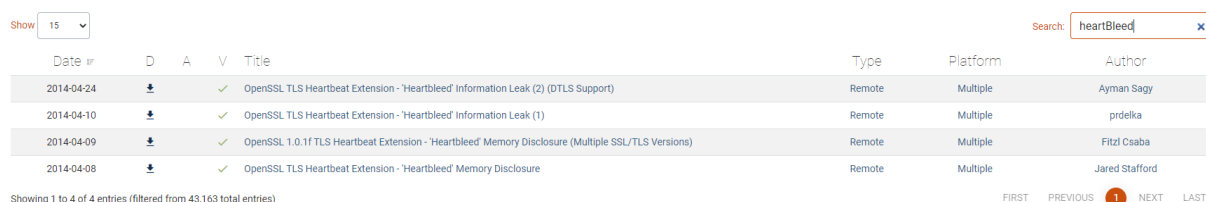
O **Heartbleed Bug** foi uma séria vulnerabilidade na famosa biblioteca OpenSSL. Esta fraquesa permitiu roubar informação protegida, que sob condições normais, por SSL/TLS encriptação usada para a segurança da internet. O SSL/TLS fornece segurança às comunicações e privacidade sobre toda as aplicações tais como a web, email e VPNs.

Este bug permitiu a que os atacantes conseguissem desviar comunicações, roubar informação diretamente dos serviços/utilizadores e falsificar este serviços/utilizadores fazendo-se passar por estes mesmos.

CVE-2014-0160 é a referência oficial para este bug e que várias versões foram afetadas :

- OpenSSL 1.0.1 através 1.0.1f (inclusive) são vulneráveis
- OpenSSL 1.0.1g não é vulnerável
- OpenSSL 1.0.0 branch não é vulnerável
- OpenSSL 0.9.8 branch não é vulnerável

Encontrei 4 exploits disponíveis ao público, no Exploit Data Base como se pode verificar na Figura 7.



The screenshot shows a search interface for 'heartBleed' on the Exploit Data Base. It displays a table with 4 entries. Each entry includes a date, a download icon, a status icon (green checkmark), a title, a type, a platform, and an author. The entries are for 'OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)', 'OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)', 'OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)', and 'OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure'.

Date	D	A	V	Title	Type	Platform	Author
2014-04-24				OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)	Remote	Multiple	Ayman Sagy
2014-04-10				OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)	Remote	Multiple	prdelka
2014-04-09				OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)	Remote	Multiple	Fitzl Csaba
2014-04-08				OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure	Remote	Multiple	Jared Stafford

Showing 1 to 4 of 4 entries (filtered from 43,163 total entries)

FIRST PREVIOUS 1 NEXT LAST

Figura 7: Alguns exploits existentes

O vetor de Ataque é representado: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N, isto é

- **Attack Vector (AV)** : Network.
- **Attack Complexity (AC)** : Baixa.
- **Privileges required (PR)** : Nenhuma.

- **User Interaction (UI)** : Nenhuma.
- **Scope (S)** : Inalterado
- **Confidentiality impact (C)** : Alta.
- **Integrity impact (I)** : Nenhuma.
- **Availability impact (A)** : Nenhuma.

Enquanto a versão vulnerável do **OpenSSL** estiver em uso, pode ser abusada. O **Fixed OpenSSL** foi lançado e tem de ser implementada ou pelos fornecedores de serviço ou até mesmo pelos utilizadores.

3 Pergunta 3

3.1 Passwords podiam ser guardadas no dicionário do teclado do telemóvel

- **CVE :** CVE-2020-15671
- **Descrição :** Quando se escrevia uma password sob certas condições, pode ter ocorrido uma *Race Condition* onde a palavra passe não foi escrita no campo certo, resultando no armazenamento da password no dicionário do teclado.
- **Versões Afetadas :** Esta vulnerabilidade afeta Firefox para Android > 80.
- **NVD Publicado :** 10/01/2020
- **Última Modificação do NVD :** 10/02/2020
- **CVSS Severity Scale :** Low (3.1)

CVSS v3.1 Severity and Metrics:

Base Score: 3.1 LOW

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

Impact Score: 1.4

Exploitability Score: 1.6

Attack Vector (AV): Network

Attack Complexity (AC): High

Privileges Required (PR): None

User Interaction (UI): Required

Scope (S): Unchanged

Confidentiality (C): Low

Integrity (I): None

Availability (A): None

Figura 8: CVSS de vulnerabilidade

3.2 As Condition Race quando lidas, certificavam a informação

- **CVE** : CVE-2020-15668
- **Descrição** : Enquanto se tentava aceder a estrutura de dados e fazer a importação do certificado de informação para uma **Database** confiável, não se conseguia adquirir o *lock*
- **Versões Afetadas** : Esta vulnerabilidade afeta o Firefox j 80 e Firefox para Android j 80.
- **NVD Publicado** : 10/01/2020
- **Última Modificação do NVD** : 10/02/2020
- **CVSS Severity Scale** : **Medium** (4.3)

CVSS v3.1 Severity and Metrics:

Base Score: 4.3 MEDIUM

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

Impact Score: 1.4

Exploitability Score: 2.8

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): Required

Scope (S): Unchanged

Confidentiality (C): Low

Integrity (I): None

Availability (A): None

Figura 9: CVSS de vulnerabilidade

3.3 Memory safety bugs fixed

- **CVE** : CVE-2020-15670
- **Descrição** : Os desenvolvedores da Mozilla reportaram alguns **bugs** na memória, descritos como *memory safe bugs*, presentes na versão 79 do Firefox para Android. Alguns destes bugs mostraram evidencia de corrupção de memória, sendo possível executar código arbitrário.
- **Versões Afetadas** : Esta vulnerabilidade afeta o Firefox j 80 e Firefox para Android j 80
- **NVD Publicado** : 10/01/2020
- **Última Modificação do NVD** : 10/02/2020
- **CVSS Severity Scale** : **High** (8.8)

CVSS v3.1 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

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 10: CVSS de vulnerabilidade

4 Pergunta 4

4.1 Download de Código sem Verificação de Integridade

Descrição: Download do código ou um executável. Este código pode ser executado sem verificar a origem e integridade do código.

Exploração: Um atacante pode executar código malicioso comprometendo o servidor host, sendo possível alterar o DNS.

4.2 Confiança nas Cookies sem Validação e Verificação da Integridade

Descrição: Certas aplicações confiam em valores de cookies em operações críticas, no entanto estas não validam nem verificam a integridades destas cookies.

Exploração: As cookies podem ser modificadas facilmente, dentro do browser ou implementando código, no lado do cliente, fora do browser. Cookies sem validação detalhada e verificação de integridade permite aos invasores autenticar-se, conduzindo a ataques como SQL injections, por exemplo.