



**Universidade do Minho**  
Escola de Engenharia

# **Segurança de Sistemas Informáticos**

**Ficha de Exercícios 1 – Vulnerabilidades e Exposições Comuns (CVE)**

**Grupo 04**

**2022/2023**

Esta ficha de exercício tem por objectivo principal apresentar a identificação padrão de vulnerabilidades e exposições publicamente conhecidas, assim como a sua importância nas atividades relacionadas com a segurança de sistemas informáticos. Espera-se, com este trabalho, promover o conhecimento de ferramentas de apoio a ações proativas de segurança.



A91697 - Luís Filipe Fernandes Vilas



A91671 - João Manuel Novais da Silva

**Prazo de submissão: 23:59 de 28/03/2023**

**Exercício 1:** Escolha três aplicações tipicamente usadas em seu computador pessoal, pesquise pela existência de vulnerabilidades conhecidas e meios de explorá-las. Descreva *detalhadamente* as descobertas, incluindo as imagens de suas pesquisas e a descrição das informações nelas contidas.

## Microsoft Word

CVE-2019-1035

Com esta vulnerabilidade descoberta, é possível correr código remotamente, assim, infectar a máquina da vítima.

VULNERABILITIES

### CVE-2019-1035 Detail

#### Description

A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1034.

#### Severity

CVSS Version 3.x

CVSS Version 2.0

##### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **7.8 HIGH**

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

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

## Google Chrome

Este ataque explora uma vulnerabilidade da biblioteca ANGLE do Google Chrome e permite acesso à heap através de uma página HTML criada.

VULNERABILITIES

### CVE-2023-1534 Detail

#### Description

Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

#### Severity

CVSS Version 3.x

CVSS Version 2.0

##### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **8.8 HIGH**

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

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

#### QUICK INFO

##### CVE Dictionary Entry:

CVE-2023-1534

##### NVD Published Date:

03/21/2023

##### NVD Last Modified:

03/23/2023

##### Source:

Chrome

Esta vulnerabilidade toma parte de um tipo de variáveis presentes no AnyDesk (no formato String) que permite a execução remota de código na máquina da vítima.

## VULNERABILITIES

## 🚩 CVE-2020-13160 Detail

## Description

AnyDesk before 5.5.3 on Linux and FreeBSD has a format string vulnerability that can be exploited for remote code execution.

## 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

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

## QUICK INFO

## CVE Dictionary Entry:

CVE-2020-13160

## NVD Published Date:

06/09/2020

## NVD Last Modified:

03/15/2021

## Source:

MITRE

**Exercício 2:** No final de 2021, foi descoberta uma falha de segurança na biblioteca open source Log4j. Esta falha foi identificada com CVE-2021-44228. 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.

## Resposta

A falha identificada acima afectava todas as versões do Log4j entre a 2.0.0 e a 2.15.0. Ela foi classificada com um Score de 10.0 pelo NVD.

O Vector de ataque desta falha era a Rede e o mesmo tinha pouca complexidade.

Existem 2 exploits revelados no site exploit-db para esta falha.

Esta vulnerabilidade teve muito impacto, pois o Log4j é amplamente usado em produção. Era possível mitigar esta vulnerabilidade, como podemos ver na imagem seguinte:

## Mitigation

For Log4j versions  $\geq 2.10$

set the system property `log4j2.formatMsgNoLookups` or the environment variable `LOG4J_FORMAT_MSG_NO_LOOKUPS` to `true`

For Log4j versions  $\geq 2.7$  and  $\leq 2.14.1$

all `PatternLayout` patterns can be modified to specify the message converter as `%m{nolookups}` instead of just `%m`

For Log4j versions  $\geq 2.0$ -beta9 and  $\leq 2.10.0$

remove the `JndiLookup` class from the classpath. For example:

### Common Vulnerability Scoring System (CVSS) Score Details

#### CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	9.8	10.0
Attack Vector	Network	Network
Attack Complexity	Low	Low
Privileges Required	None	None
User Interaction	None	None
Scope	Unchanged	Changed
Confidentiality Impact	High	High
Integrity Impact	High	High
Availability Impact	High	High

#### CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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

## Exploit Database Advanced Search

Title

CVE

Type

Platform

Port

Content

Author

Tag

☐ Verified ☐ Has App ☐ No Metasploit

Show 15

Date	D	A	V	Title	Type	Platform	Author
2021-12-14				Apache Log4j2 2.14.1 - Information Disclosure	remote	Java	leonjza
2021-12-14				Apache Log4j 2 - Remote Code Execution (RCE)	remote	Java	kozmer

**Exercício 3:** 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.

## Resposta

Esta falha foi classificada pelo NIST (NVD) com 7.5 segundo a escala CVSS 3.x. Afectou as versões 1.0.1 a 1.0.1f e 1.0.2-beta.

A falha permitia ao atacante, obter 64k da memória da vítima, a cada chamada. A solução encontrada, foi a atualização para a versão 1.0.1g. O vector de ataque é, novamente a Rede e, segundo o exploit-db.com existem os seguintes exploits:

Title

Title

CVE

2014-0160

Type

Platform

Port

Content

Exploit content

Author

Author

Tag

Search

☐ Verified

☐ Has App

☐ No Metasploit

Reset All

Show

15

Date	#	D	A	V	Title	Type	Platform	Author
2020-12-22					HeartBleed Attack - Paper	papers	Multiple	Jaspreet Singh
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

# OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)

Last Revised: October 05, 2016

Alert Code: TA14-098A



## Systems Affected

- OpenSSL 1.0.1 through 1.0.1f
- OpenSSL 1.0.2-beta

## Overview

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.

OpenSSL versions 1.0.1 through 1.0.1f contain a flaw in its implementation of the TLS/DTLS heartbeat functionality. This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time. Note that an attacker can repeatedly leverage the vulnerability to retrieve as many 64k chunks of memory as are necessary to retrieve the intended secrets. The sensitive

## Impact

Essa falha permite que um invasor remoto recupere a memória privada de um aplicativo que usa a biblioteca OpenSSL vulnerável em blocos de 64k de cada vez.

## Solution

[OpenSSL 1.0.1g](#) has been released to address this vulnerability. Any keys generated with a vulnerable version of OpenSSL should be considered compromised and regenerated and deployed after the patch has been applied.

US-CERT recommends system administrators consider implementing [Perfect Forward Secrecy](#) to mitigate the damage that may be caused by future private key disclosures.

**Exercício 4:** Assim como diversas corporações, a Mozilla Foundation divulga informações sobre vulnerabilidades para as quais os seus produtos foram expostos através do seu Security Advisories. Em 14 de Março de 2023, a companhia disponibilizou uma atualização do seu browser, *i.e.*, Firefox ESR 102.9. Esta versão resolve uma série de vulnerabilidades listadas no relatório [MFSA 2023-10](#). Descreva *detalhadamente* duas vulnerabilidades listadas neste relatório e identificada como de possível alto impacto (*i.e.*, *high*).

## Resposta

Encontramos pelo menos duas vulnerabilidades identificadas como de possível alto impacto. Ambas as vulnerabilidades eram exploradas através da Rede.

Entre elas:

CVE-2023-25751

A vulnerabilidade encontrada é usada quando se invalida o código JIT, quando segue um iterador. Não existe nenhum exploit encontrado até ao momento no exploit-db.com.

## CVE-2023-25751

Public on 14 de março de 2023

Last Modified: 27 de março de 2023 às 21:38:10 UTC



**Important Impact**  
[What does this mean?](#)

7.5

[CVSS v3 Base Score](#)  
CVSS Score Breakdown

### Description

A flaw was found in Mozilla. The Mozilla Foundation Security Advisory describes the issue of invalidating JIT code while following an iterator. The newly generated code could be overwritten incorrectly, leading to a potentially exploitable crash.

### Statement


Red Hat Product Security rates the severity of this flaw as determined by the Mozilla Foundation Security Advisory.

## CVE-2023-28176

Esta falha apareceu após terem sido encontrados bugs de segurança na memória. Afectou o Firefox 110 e ESR 102.8. Segundo a Mozilla, com algum esforço seria possível executar código arbitrário. Apesar disso, não foram encontrados, ainda, exploits no exploit-db.com

### CVE-2023-28176

Public on 14 de março de 2023  
Last Modified: 27 de março de 2023 às 21:38:28 UTC



**Important Impact**  
[What does this mean?](#)

7.5

[CVSS v3 Base Score](#)  
CVSS Score Breakdown

### Description

A flaw was found in Mozilla. The Mozilla Foundation Security Advisory described the issue in which Mozilla developers Timothy Nikkel, Andrew McCreight, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 110 and ESR 102.8. 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.

### Statement

Red Hat Product Security rates the severity of this flaw as determined by the Mozilla Foundation Security Advisory.

**Exercício 5:** Recorrendo ao CWE, descreva três tipos comuns de problemas relacionados com integridade de dados identificados no desenvolvimento de software e como podem ser evitados.

## Resposta

Exemplos de problemas relacionados com a integridade dos dados identificados no desenvolvimento de software podem ser:

- ➔ Problemas de Encapsulamento
  - Pode ser resolvido, aprendendo técnicas de encapsulamento da informação
- ➔ Problemas de Validação da Informação
  - Pode ser evitado, se verificarmos toda a informação recebida pelo cliente
- ➔ Más praticas de código
  - Pode ser resolvido se o código for estruturado de uma melhor forma.