

Ficha 01

Ana Margarida Campos A85166

20 de Outubro de 2020

1 Resolução

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 suas descobertas, incluindo as imagens de suas pesquisas e a descrição das informações nelas contidas.

Resposta: As três aplicações selecionadas são Blackboard, Spotify e MySQL. De seguida é mostrado, para cada uma das três aplicações, um conjunto alargado de vulnerabilidades identificadas bem como meios de as explorar. Uma vez que as listas de vulnerabilidades são grandes, foi escolhida uma vulnerabilidade de cada aplicação para ser abordada detalhadamente.

Blackboard

Search Results	
There are 24 CVE entries that match your search.	
Name	Description
CVE-2020-9008	Stored Cross-site scripting (XSS) vulnerability in Blackboard Learn/PeopleTool v9.1 allows users to inject arbitrary web script via the Tile widget in the People Tool profile editor.
CVE-2018-13257	The bb-auth-provider-cas authentication module within Blackboard Learn 2018-07-02 is susceptible to HTTP host header spoofing during Central Authentication Service (CAS) service ticket validation, enabling a phishing attack from the CAS server login page.
CVE-2017-18262	Blackboard Learn (Since at least 17th of October 2017) has allowed Unvalidated Redirects on any signed-in user through its endpoints for handling Shibboleth logins, as demonstrated by a webapps/bb-auth-provider-shibboleth-BBLEARN/execute/shibbolethLogin?returnUrl= URI.
CVE-2014-0811	Cross-site scripting (XSS) vulnerability in Blackboard Vista/CE 8.0 SP6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2010-3245	The automated-backup functionality in Blackboard Transact Suite (formerly Blackboard Commerce Suite) stores the (1) database username and (2) database password in cleartext in (a) script and (b) batch (.bat) files, which allows local users to obtain sensitive information by reading a file.
CVE-2010-3244	BitsConnection_Edit.exe in Blackboard Transact Suite (formerly Blackboard Commerce Suite) before 3.6.0.2 relies on field names when determining whether it is appropriate to decrypt a connection.xml field value, which allows local users to discover the database password via a modified connection.xml file that contains an encrypted password in the <Server> field.
CVE-2008-3421	Multiple cross-site request forgery (CSRF) vulnerabilities in Blackboard Academic Suite 8.0.260.7 allow remote attackers to hijack the authentication of student users for requests that change configuration and enrollments via unspecified input to (1) update_module.jsp, (2) enroll_course.pl, and (3) unenroll.jsp.
CVE-2008-1883	The server in Blackboard Academic Suite 7.x stores MD5 password hashes that are provided directly by clients, which makes it easier for remote attackers to access accounts via a modified client that skips the javascript/md5.js hash calculation, and instead sends an arbitrary MD5 string.
CVE-2008-1795	Multiple cross-site scripting (XSS) vulnerabilities in Blackboard Academic Suite 7.x and earlier, and possibly some 8.0 versions, allow remote attackers to inject arbitrary web script or HTML via (1) the searchText parameter in a Course action to webapps/blackboard/execute/viewCatalog or (2) the data__announcements__pk1_pk2__subject parameter in an ADD action to bin/common/announcement.pl.
CVE-2008-0750	SQL injection vulnerability in philboard_forum.asp in Huxrev BlackBoard 2.0.2 allows remote attackers to execute arbitrary SQL commands via the forumid parameter.
CVE-2007-5227	Multiple cross-site scripting (XSS) vulnerabilities in messaging/course/composeMessage.jsp in Blackboard Learning System 6.3.1.593 and earlier in Blackboard Academic Suite allow remote attackers to inject arbitrary web script or HTML via the (1) subject_t and (2) body_text parameters. NOTE: vector 2 requires bypassing a client-side security mechanism that attempts to block XSS sequences.
CVE-2006-4308	Multiple cross-site scripting (XSS) vulnerabilities in Blackboard Learning System 6, Blackboard Learning and Community Portal Suite 6.2.3.23, and Blackboard Vista 4 allow remote attackers to inject arbitrary JavaScript, VBScript, or HTML via (1) data, (2) vbscript, and (3) malformed javascript URIs in various HTML tags when posting to the Discussion Board.
CVE-2006-3914	Cross-site scripting (XSS) vulnerability in Blackboard Academic Suite 6.2.3.23 allows remote authenticated users to inject arbitrary HTML or web script by bypassing client-side validation through disabling JavaScript when submitting an essay response, which has no server-side validation before being viewed via "View Attempt Details" in the Gradebook.

Figura 1: Algumas vulnerabilidades da aplicação Blackboard segundo CVE

Search Parameters:		There are 24 matching records. Displaying matches 1 through 20.	
<ul style="list-style-type: none">Results Type: OverviewKeyword (text search): blackboardSearch Type: Search All			1 2 > >>
Vuln ID 基	Summary ①	CVSS Severity ②	
CVE-2020-9008	Stored Cross-site scripting (XSS) vulnerability in Blackboard Learn/PeopleTool v9.1 allows users to inject arbitrary web script via the Tile widget in the People Tool profile editor. Published: Fevereiro 25, 2020; 1:15:11 PM -0500	V3.1: 5.4 MEDIUM V2.0: 3.5 LOW	
CVE-2018-13257	The bb-auth-provider-cas authentication module within Blackboard Learn 2018-07-02 is susceptible to HTTP host header spoofing during Central Authentication Service (CAS) service ticket validation, enabling a phishing attack from the CAS server login page. Published: Novembro 18, 2019; 11:15:11 AM -0500	V3.1: 6.1 MEDIUM V2.0: 5.8 MEDIUM	
CVE-2017-18262	Blackboard Learn (Since at least 17th of October 2017) has allowed Unvalidated Redirects on any signed-in user through its endpoints for handling Shibboleth logins, as demonstrated by a webapps/bb-auth-provider-shibboleth-BBLEARN/execute/shibbolethLogin?returnUrl= URI. Published: Abril 30, 2018; 9:29:00 AM -0400	V3.0: 6.1 MEDIUM V2.0: 5.8 MEDIUM	
CVE-2014-0811	Cross-site scripting (XSS) vulnerability in Blackboard Vista/CE 8.0 SP6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. Published: Fevereiro 22, 2014; 4:55:09 PM -0500	V3.x:(not available) V2.0: 4.3 MEDIUM	

Figura 2: Algumas vulnerabilidades da aplicação Blackboard segundo NVD

Date	IF	D	A	V	Title	Type	Platform	Author
2017-01-09					Blackboard LMS 9.1 SP14 - Cross-Site Scripting	WebApps	Java	Vulnerability-Lab
2011-05-25					BlackBoard Learn 8.0 - 'keywordraw' Cross-Site Scripting	WebApps	CGI	Matt Jezorek
2008-03-26					BlackBoard Academic Suite 6/7 - '/bin/common/announcement.pl?data__announcements__pk1_pk2__subject' Cross-Site Scripting	WebApps	CGI	Knight4vn
2008-03-26					BlackBoard Academic Suite 6/7 - '/webapps/BlackBoard/execute/viewCatalog?searchText' Cross-Site Scripting	WebApps	CGI	Knight4vn
2006-08-24					BlackBoard Products 6 - Multiple HTML Injection Vulnerabilities	WebApps	PHP	proton
2005-12-12					BlackBoard Academic Suite 6.2.3.23 - Frameset.jsp Cross-Domain Frameset Loading	WebApps	JSP	dr_insane
2004-10-06					BlackBoard Internet NewsBoard System 1.5.1 - Remote File Inclusion	WebApps	PHP	Lin Xiaofeng
2004-06-10					BlackBoard Learning System 6.0 - Dropbox File Download	WebApps	CGI	Maarten Verbeek
2004-04-12					BlackBoard Learning System 5.x/6.0 - Multiple Cross-Site Scripting Vulnerabilities	WebApps	CGI	DarC KonQuest
2002-07-01					BlackBoard 5.0 - Cross-Site Scripting	WebApps	CGI	Berend-Jan Wever

Figura 3: Conjunto de exploits para a aplicação Blackboard

Vulnerabilidade: CVE-2020-9008

Uma das vulnerabilidades da aplicação **Blackboard** versão 9.1 consiste em *Stored Cross-site scripting (XSS)*. Esta vulnerabilidade permite aos utilizadores injetar *web scripts* arbitrários ao aceder ao seu perfil.

De acordo com a figura seguinte podemos constatar que o ataque é realizado a partir da rede e que se trata de um ataque de complexidade média. O nível de comprometer a confidencialidade é baixo.

CVSS v3.1 Severity and Metrics:

Base Score: 5.4 MEDIUM

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

Impact Score: 2.7

Exploitability Score: 2.3

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): Low

User Interaction (UI): Required

Scope (S): Changed

Confidentiality (C): Low

Integrity (I): Low

Availability (A): None

Spotify

Search Results

There are 3 CVE entries that match your search.

Name	Description
CVE-2018-1167	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.
CVE-2018-1000843	Luigi version prior to version 2.8.0; after commit 53b52e12745075a8acc016d33945d9d6a7a6aaeb; after GitHub PR spotify/luigi/pull/1870 contains a Cross Site Request Forgery (CSRF) vulnerability in API endpoint: /api/<method> that can result in Task metadata such as task name, id, parameter, etc. will be leaked to unauthorized users. This attack appear to be exploitable via The victim must visit a specially crafted webpage from the network where their Luigi server is accessible.. This vulnerability appears to have been fixed in 2.8.0 and later.
CVE-2017-17750	Bose SoundTouch devices allow XSS via a crafted public playlist from Spotify.

Figura 4: Algumas vulnerabilidades da aplicação Spotify segundo CVE

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): spotify
- Search Type: Search All

There are 4 matching records.
Displaying matches 1 through 4.

Vuln ID	Summary	CVSS Severity
CVE-2020-6841	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. Published: Fevereiro 21, 2020; 11:15:11 AM -0500	V3.1: 9.8 CRITICAL V2.0: 10.0 HIGH
CVE-2018-1000843	Luigi version prior to version 2.8.0; after commit 53b52e12745075a8acc016d33945d9d6a7a6aaeb; after GitHub PR spotify/luigi/pull/1870 contains a Cross Site Request Forgery (CSRF) vulnerability in API endpoint: /api/<method> that can result in Task metadata such as task name, id, parameter, etc. will be leaked to unauthorized users. This attack appear to be exploitable via The victim must visit a specially crafted webpage from the network where their Luigi server is accessible.. This vulnerability appears to have been fixed in 2.8.0 and later. Published: Dezembro 20, 2018; 10:29:02 AM -0500	V3.0: 8.8 HIGH V2.0: 6.8 MEDIUM
CVE-2018-1167	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. Published: Abril 18, 2018; 10:29:00 PM -0400	V3.0: 8.8 HIGH V2.0: 6.8 MEDIUM
CVE-2017-17750	Bose SoundTouch devices allow XSS via a crafted public playlist from Spotify. Published: Março 24, 2018; 2:29:00 PM -0400	V3.0: 5.4 MEDIUM V2.0: 3.5 LOW

Figura 5: Algumas vulnerabilidades da aplicação Spotify segundo NVD

Date	D	A	V	Title	Type	Platform	Author
2019-01-16				Spotify 1.0.96.181 - 'Proxy configuration' Denial of Service (PoC)	DoS	Windows	Aaron V. Hernandez
2012-03-23				Spotify 0.8.2.610 - search func Memory Exhaustion	DoS	Windows	LiquidWorm

Figura 6: Conjunto de exploits para a aplicação Spotify

Vulnerabilidade: CVE-2018-1167

Na versão 1.0.69.336 da aplicação Spotify existe uma vulnerabilidade que permite aos atacantes executar código arbitrário de modo a que um utilizador comum visite uma página ou abra um ficheiro malicioso. O problema resulta da falta de validação adequada de uma string fornecida pelo utilizador antes de usá-la para executar uma chamada de sistema.

De acordo com a figura seguinte podemos constatar que o ataque é realizado a partir da rede e que se trata de um ataque de complexidade elevada. O nível de comprometer a confidencialidade é bastante elevado.

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

MySQL

Search Results	
There are 1250 CVE entries that match your search.	
Name	Description
CVE-2020-9483	**Resolved** When use H2/MySQL/TiDB as Apache SkyWalking storage, the metadata query through GraphQL protocol, there is a SQL injection vulnerability, which allows to access unexpected data. Apache SkyWalking 6.0.0 to 6.6.0, 7.0.0 H2/MySQL/TiDB storage Implementations don't use the appropriate way to set SQL parameters.
CVE-2020-8611	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, multiple SQL Injection vulnerabilities have been found in the REST API that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database via the REST API. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or destroy database elements.
CVE-2020-8521	SQL injection with start and length parameters in Records.php for phpzag live add edit delete data tables records with ajax.php.mysql
CVE-2020-8520	SQL injection in order and column parameters in Records.php for phpzag live add edit delete data tables records with ajax.php.mysql
CVE-2020-8519	SQL injection with the search parameter in Records.php for phpzag live add edit delete data tables records with ajax.php.mysql
CVE-2020-8505	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=deletedadmin CSRF to delete a user.
CVE-2020-8504	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=deletedadmin CSRF to add an administrative user.
CVE-2020-7221	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.
CVE-2020-5777	MAGMI versions prior to 0.7.24 are vulnerable to a remote authentication bypass due to allowing default credentials in the event there is a database connection failure. A remote attacker can trigger this connection failure if the Mysql setting max_connections (default 151) is lower than Apache (or another web server) setting MaxRequestWorkers (formerly MaxClients) (default 256). This can be done by sending at least 151 simultaneous requests to the Magento website to trigger a "Too many connections" error, then use default magmi:magmi basic authentication to remotely bypass authentication.
CVE-2020-5504	In phpMyAdmin 4 before 4.9.4 and 5 before 5.0.1, SQL injection exists in the user accounts page. A malicious user could inject custom SQL in place of their own username when creating queries to this page. An attacker must have a valid MySQL account to access the server.
CVE-2020-5399	Cloud Foundry CredHub, versions prior to 2.5.10, connects to a MySQL database without TLS even when configured to use TLS. A malicious user with access to the network between CredHub and its MySQL database may eavesdrop on database connections and thereby gain unauthorized access to CredHub and other components.
CVE-2020-2934	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.19 and prior and 5.1.48 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L).

Figura 7: Algumas vulnerabilidades da aplicação MySQL segundo CVE

Q

Search Results

(Refine Search)

Sort results by:

Publish Date Descending

Sort

Search Parameters:

• Results Type: Overview

• Keyword (text search): mysql

• Search Type: Search All

There are 1,312 matching records.

Displaying matches 1 through 20.

1

2

3

4

5

6

7

8

9

10

>

>>

Vuln ID	Summary	CVSS Severity
CVE-2020-23832	<p>A Persistent Cross-Site Scripting (XSS) vulnerability in message_admin.php in Projectworlds Car Rental Management System v1.0 allows unauthenticated remote attackers to harvest an admin login session cookie and steal an admin session upon an admin login.</p> <p>Published: Outubro 06, 2020; 9:15:13 AM -0400</p>	<div>V3.1: 6.1 MEDIUM</div> <div>V2.0: 4.3 MEDIUM</div>
CVE-2020-14027	<p>An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The database connection strings accept custom unsafe arguments, such as ENABLE_LOCAL_INFILTE, that can be leveraged by attackers to enable MySQL Load Data Local (rogue MySQL server) attacks.</p> <p>Published: Setembro 22, 2020; 2:15:23 PM -0400</p>	<div>V3.1: 5.3 MEDIUM</div> <div>V2.0: 3.5 LOW</div>
CVE-2020-25487	<p>PHPGURUKUL Zoo Management System Using PHP and MySQL version 1.0 is affected by: SQL Injection via zms/animal-detail.php.</p> <p>Published: Setembro 22, 2020; 1:15:12 PM -0400</p>	<div>V3.1: 7.8 HIGH</div> <div>V2.0: 4.6 MEDIUM</div>
CVE-2019-20917	<p>An issue was discovered in InspIRCd 2 before 2.0.28 and 3 before 3.3.0. The mysql module contains a NULL pointer dereference when built against mariadb-connector-c 3.0.5 or newer. When combined with the sqlauth or sqloper modules, this vulnerability can be used for remote crashing of an InspIRCd server by any user able to connect to a server.</p> <p>Published: Setembro 11, 2020; 1:15:12 AM -0400</p>	<div>V3.1: 6.5 MEDIUM</div> <div>V2.0: 6.8 MEDIUM</div>

Figura 8: Algumas vulnerabilidades da aplicação MySQL segundo NVD

Date	D	A	V	Title	Type	Platform	Author
2018-04-18				MySQL Squid Access Report 2.1.4 - SQL Injection / Cross-Site Scripting	WebApps	PHP	Keerati T.
2017-05-01				MySQL < 5.6.35 / < 5.7.17 - Integer Overflow	DoS	Multiple	Rodrigo Marcos
2013-03-07				MySQL / MariaDB - Geometry Query Denial of Service	DoS	Linux	Alyssa Milburn
2012-12-06				Oracle MySQL / MariaDB - Insecure Salt Generation Security Bypass	Remote	Linux	kingcope
2012-04-27				MySQLDumper 1.24.4 - 'menu.php' PHP Remote Code Execution	WebApps	PHP	AkaStep
2012-04-27				MySQLDumper 1.24.4 - 'index.php?page' Cross-Site Scripting	WebApps	PHP	AkaStep
2012-04-27				MySQLDumper 1.24.4 - 'main.php' Multiple Cross-Site Request Forgery Vulnerabilities	WebApps	PHP	AkaStep
2012-04-27				MySQLDumper 1.24.4 - Multiple Script Direct Request Information Disclosures	WebApps	PHP	AkaStep

Figura 9: Conjunto de exploits para a aplicação MySQL

Vulnerabilidade: CVE-2020-8611

Nesta vulnerabilidade foram encontradas na API REST várias falhas de injeção SQL que podem permitir que um atacante autenticado obtenha acesso não autorizado ao banco de dados do MOVEit Transfer. O atacante pode ser capaz de inferir informações sobre a estrutura e o conteúdo da base de dados e ainda executar instruções SQL que alteram ou destroem dados. De acordo com a figura seguinte podemos constatar que o ataque é realizado a partir da rede e que se trata de um ataque de complexidade elevada. O nível de comprometer a confidencialidade é bastante elevado.

CVSS v3.1 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/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): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Exercício 2: 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:

CVE-ID
CVE-2014-0160 Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
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 10: Vulnerabilidade Heartbleed

De acordo com a Figura 10 a falha conhecida como *Heartbleed* afetou as versões que vão desde a versão 1.0.1 até à versão 1.0.1g. Esta vulnerabilidade ocorreu uma vez que as implementações TLS e DTLS do OpenSSL não manipulavam corretamente os pacotes de extensão da Heartbeat. Isto permitia que os atacantes remotos obtivessem informações confidenciais da memória do processo a partir de pacotes que ativavam o *buffer-over-read*. Os exploits existentes são mostrados na figura seguinte.

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

Figura 11: Conjunto de exploits Heartbleed

Na próxima figura é possível ver algumas informações pertinentes tais como os vestores de ataque.

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

De acordo com a figura, esta vulnerabilidade apresenta um impacto relativamente elevado e com exposição elevada da confidencialidade.

De maneira a anular esta vulnerabilidade é necessário fazer a atualização do server para a versão 1.01g ou superior uma vez que esta falha foi estagnada a partir desta versão.

Exercício 3: 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 MFSA 2020-39. Descreva detalhadamente três vulnerabilidades listadas neste relatório.

Resposta: Três vulnerabilidades listadas no relatório MFSA 2020-39 são:

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

Reporter Kaizer Soze


Impact  high

Figura 12: Vulnerabilidade CVE-2020-15664

Esta vulnerabilidade poderia solicitar ao utilizador a instalação de uma extensão não intencional ou maliciosa. Isto acontecia devido ao facto da referência à função `eval()` estar na janela `about:blank`, o que permitiria a uma *webpage* perigosa ter acesso ao objeto *InstallTrigger* que iria solicitar ao utilizador a instalação da tal extensão.

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

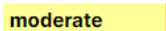
Impact  moderate

Figura 13: Vulnerabilidade CVE-2020-12401

Esta vulnerabilidade ocorreu durante a geração da assinatura ECDSA. Consistiu em deixar de assegurar a multiplicação escalar em tempo constante. Isto resultou na execução em tempo variável de alguns dados secretos.

CVE-2020-12400: P-384 and P-521 vulnerable to a side channel attack on modular inversion

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

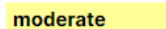
Impact  moderate

Figura 14: Vulnerabilidade CVE-2020-12400

Esta vulnerabilidade ocorria ao converter coordenadas cartesianas noutro tipo de coordenadas (*affine coordinates*). A inversão modular não era realizado em tempo constante, o que permitiria que existisse um ataque baseado no tempo no canal.

Exercício 4: Recorrendo ao CWE, descreva dois tipos comuns de problemas relacionados com integridade de dados identificados no desenvolvimento de software.

Resposta: A integridade de dados consiste em assegurar a autenticidade da informação, ou seja, os dados devem ser mantidos e confiáveis ao longo de todo o seu ciclo de vida.

De acordo com o CWE, dois tipos de problemas relacionados com a integridade no desenvolvimento de software são a utilização de cookies sem validação e verificação de integridade e, o outro problema centra-se no design e arquitetura dos componentes do sistema, como mensagens e ficheiros, garantirem integridade.

CWE-565: Reliance on Cookies without Validation and Integrity Checking

Weakness ID: 565
Abstraction: Base
Structure: Simple

Status: Incomplete

Assentando no primeiro problema, caso não exista uma validação detalhada e verificação de integridade nas cookies, os invasores podem ignorar a autenticação e conduzir a ataques de injeção (como injeção de SQL e scripts entre sites) modificando e implementado código não autorizado.

CWE CATEGORY: Verify Message Integrity

Category ID: 1020

Status: Draft

No caso do segundo problema, o facto de não ser projetada e implementada uma arquitetura segura leva a uma degradação da qualidade e da integridade dos dados.