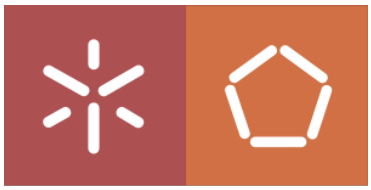


Universidade do Minho
Escola de Engenharia

Universidade do Minho
Mestrado Integrado em Engenharia Informática

SSI

Segurança de Sistemas Informáticos
Ficha 1

Outubro 2020

Tânia Filipa Amorim Rocha
A85176

1 Pergunta 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.

As aplicações escolhidas para esta pesquisa foram:

- SoundCloud
- EpicGames Laucher
- UberEATS

Primeiramente, analisando o caso da aplicação de upload e streaming de música, nomeadamente um dos existentes plugins para utilização da aplicação mais rapidamente com atalhos entre listas de reprodução e áudios.

Na versão deste plugin nomeada de Soundcloud is Gold 2.1 foi descoberta uma vulnerabilidade de segurança quando ao cruzamento de dados pessoais entre sites. Isto devido à falha desta versão de limpar o input fornecido pelos utilizadores.

Esta vulnerabilidade de segurança pode ser aproveitada para ataques externos sem a suspeita do utilizador, na medida em que esta falha permite a um atacante roubar as cookies responsáveis pelas credenciais de autenticação que, permitirão ataques em outros sites de um mesmo utilizador. O id desta vulnerabilidade é CVE-2012-6624.

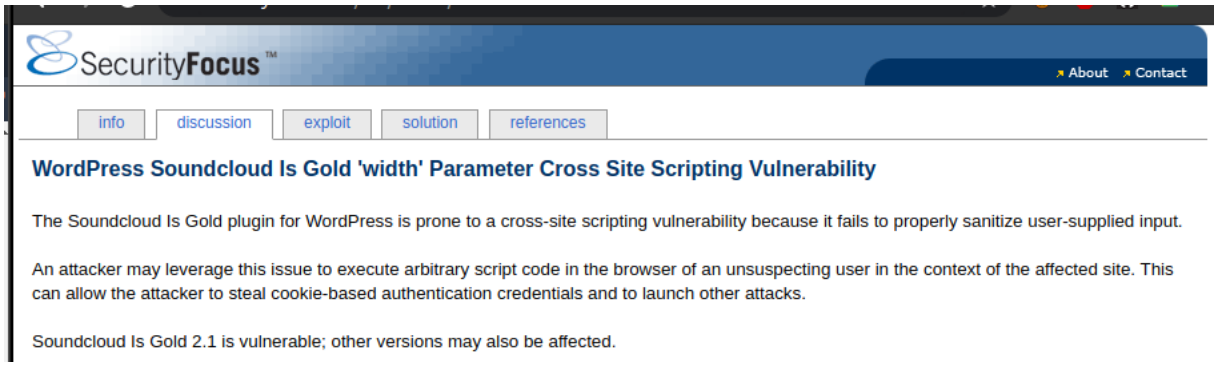


Figura 1: descrição da vulnerabilidade da aplicação do Souncloud.

No caso da aplicação EpicGames em versões anteriores à 8.2.2, alguns launcher da instalação da aplicação possuem uma vulnerabilidade que pode ser utilizada por atacantes com a utilização de um URL construída com o propósito de levar o utilizador a visitar sites ou ficheiros maliciosos. Esta vulnerabilidade foi considerada de Alta categoria, o que remete a uma falha muito grave em termos de segurança do utilizador. o id desta vulnerabilidade é CVE-2018-17707.

Por fim, no caso da aplicação mobile para iOS UberEATS foi encontrada uma vulnerabilidade nas chaves de encriptação, que permite a qualquer utilizador com acesso uma das keys ter acesso à data armazenada nessa mesma key. O id desta vulnerabilidade é CVE-2017-13104.

Description

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Epic Games Launcher versions prior to 8.2.2. 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 handler for the com.epicgames.launcher protocol. A crafted URI with the com.epicgames.launcher protocol can trigger execution of a system call composed from a user-supplied string. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-7241.

Figura 2: descrição da vulnerabilidade do laucher da aplicação EpicGames.

Description

Uber Technologies, Inc. UberEATS: Uber for Food Delivery, 1.108.10001, 2017-11-02, iOS application uses a hard-coded key for encryption. Data stored using this key can be decrypted by anyone able to access this key.

Figura 3: descrição da vulnerabilidade da aplicação do UberEATS.

2 Pergunta 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.

A falha em questão, nomeada de "heartbleed", é uma vulnerabilidade que permite o roubo de informação protegida que, em condições normais, deveria assegurar a Internet através da encriptação SSL/TLS. Esta encriptação fornece segurança e privacidade na comunicação na Internet em aplicações como email, web e outras networks privadas.

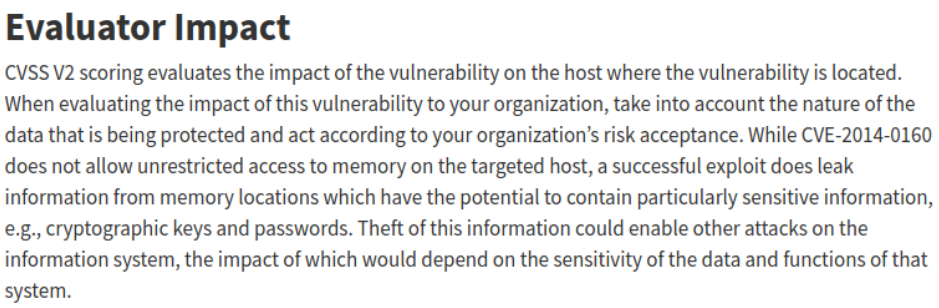
Esta falha permite a qualquer pessoa na Internet ler a memoria dos sistemas protegidos das versões vulneráveis do software o que compromete as keys privadas utilizadas para a encriptação de nomes, password, conteudo pessoal, comunicações e até mesmo roubar data diretamente de serviços e utilizadores.

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 4: descrição da vulnerabilidade HeartBleed.

O impacto desta vulnerabilidade é de grande dimensão visto que, grandes servidores web foram afetados e é possivel que até o cidadão comum tenha sido direta ou indiretamente afetado e é qualquer ataque tem o seu registo completamente apagado.



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 5: Impacto do bug Hearbleed.

Existem várias versões afectadas por este bug desde a versão do OpenSSL 1.0.1 até 1.0.1g.

Até alguns sistemas operativos podem ter sido exportados com esta falha nas suas versões OpenSSL como por exemplo Debian Wheezy, Ubunto 12.04.4 LTS entre outros.

Vulnerable:

Ubuntu Ubuntu Linux 12.04 LTS i386
Ubuntu Ubuntu Linux 12.04 LTS amd64
Red Hat Enterprise Virtualization Hypervisor for RHEL 6 0
Red Hat Enterprise Linux Workstation Optional 6
Red Hat Enterprise Linux Workstation 6
Red Hat Enterprise Linux Server Optional 6
Red Hat Enterprise Linux Server 6
Red Hat Enterprise Linux HPC Node Optional 6

Figura 6: Sistemas Operativos e software afectados

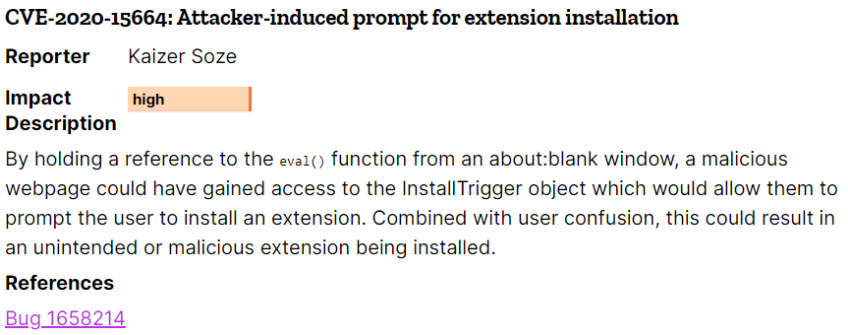
Uma das soluções para este bug seria resolver directamente o código, no entanto, apesar de profissionais terem trabalhado nesta solução, a utilização de versões mais recentes e seguras é recomendada.

3 Pergunta 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.

Este relatório apresenta detalhadamente todas as vulnerabilidades resolvidas na actualização do browser, 3 delas que serão analisadas foram:

- CVE-2020-15664. Esta vulnerabilidade tinha origem numa referencia numa função *eval()* assecivel de uma página about:blank que continha uma webpage maligna que iniciaria automaticamente umas instalação de uma extensão maligna.

  Esta vulnerabilidade considerada de severity 6.5 média afecta várias versões do browser firefox e tem um impacto considerado alto.


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

Reporter Kaizer Soze

Impact high

Description

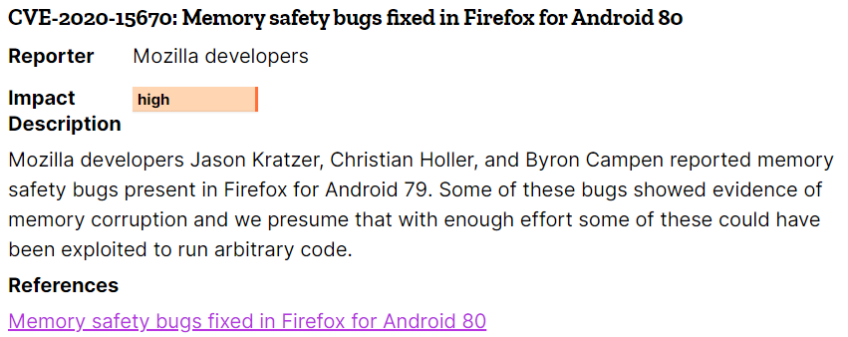
By holding a reference to the `eval()` function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension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

References

Bug 1658214

Figura 7: Vulnerabilidade CVE-2020-15664

- CVE-2020-15670. Um bug que afectava a segurança da memória presente no firebox para android 79. Este bug apresentava evidencia de corrupção de memória e poderá ter sido usado para executar código exterior. Esta vulnerabilidade foi considerada com uma severidade alta de 8.8 e de impacto alto.


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.

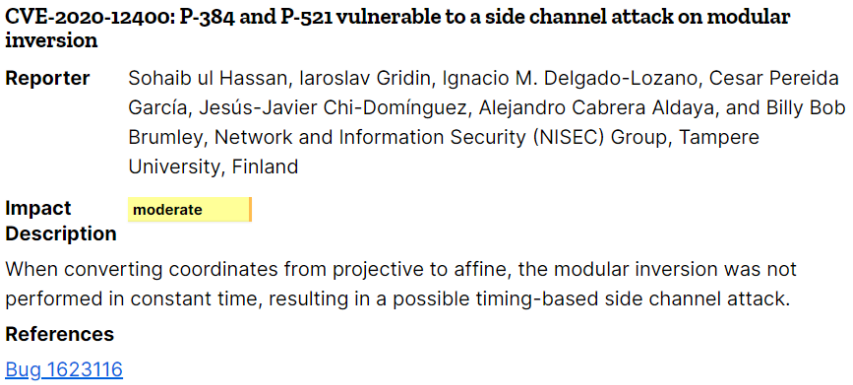
References

Memory safety bugs fixed in Firefox for Android 80

Figura 8: Vulnerabilidade CVE-2020-15670

- CVE-2020-12400. Esta vulnerabilidade consiste aquando da conversão de coordenadas em que a inversão modular não era feita em tempo constante o que poderia causar canais de

ataque baseados nesta falha de tempo. Esta vulnerabilidade afecta as versões do firefox e firefox android anteriores a 80, tem uma severidade avaliada em 4.7, isto é, média e um impacto moderado.



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

Description

When converting coordinates from projective to affine, the modular inversion was not performed in constant time, resulting in a possible timing-based side channel attack.

References

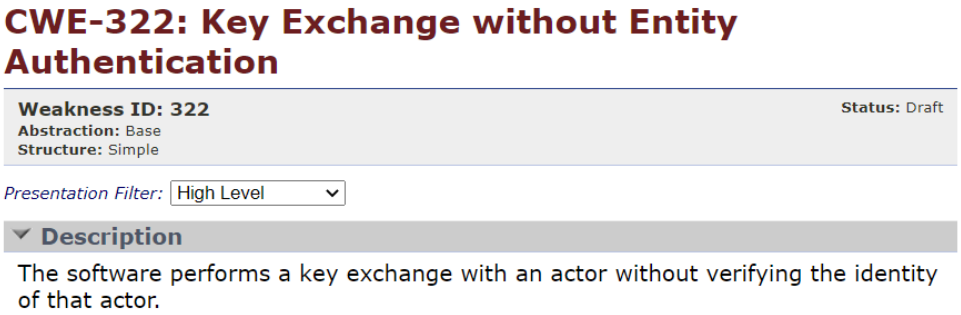
Bug 1623116

Figura 9: Vulnerabilidade CVE-2020-12400

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

Após uma pequena pesquisa recorrendo ao CWE, os dois problemas comuns escolhidos relacionados com a integridade de dados no desenvolvimento de software foram:

- CWE-322. Esta "fraqueza"está relaciona com a troca de chaves sem autentificar o utilizador em questão. A troca de chaves entre entidades é uma forma de preservar a integridade da informação enviada entre elas, no entanto nada garante que estas entidades são realmente quem apresentam ser o que pode permitir ataques através de identidade não verdadeira e assim controlar as troca de dados.



CWE-322: Key Exchange without Entity Authentication

Weakness ID: 322 **Status:** Draft
Abstraction: Base
Structure: Simple

Presentation Filter: High Level

Description

The software performs a key exchange with an actor without verifying the identity of that actor.

Figura 10: Fraqueza CWE-322

- CWE-348: Uma outra "fraqueza"no desenvolvimento de um software são as sources da informação aí disponível. Por exemplo quando este software tem duas ou mais sources diferentes do mesmo tipo de informação mas usa a source menos confiável ou seja, neste caso, a que é menos resistente a um ataque exterior.

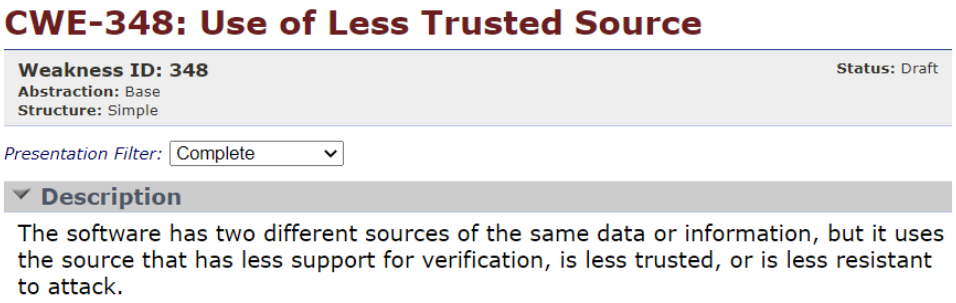


Figura 11: Fraqueza CWE-348

5 Bibliografia

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6624

https://www.securityfocus.com/bid/53537/info

https://www.exploit-db.com/exploits/37203

https://www.zerodayinitiative.com/advisories/ZDI-18-1359/

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17707

https://nvd.nist.gov/vuln/detail/CVE-2018-17707vulnCurrentDescriptionTitle

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13104

https://nvd.nist.gov/vuln/detail/CVE-2017-13104

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

https://nvd.nist.gov/vuln/detail/CVE-2014-0160

https://support.f5.com/csp/article/K15159

https://heartbleed.com/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-39/

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15664

https://nvd.nist.gov/vuln/detail/CVE-2020-15664vulnCurrentDescriptionTitle

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15670

https://nvd.nist.gov/vuln/detail/CVE-2020-15670

https://cwe.mitre.org/data/definitions/699.html

https://cwe.mitre.org/data/definitions/322.html