Tecnologia de Segurança (4º ano de Engenharia Informática)

Trabalho Prático Nº1

Relatório de Desenvolvimento

Carla Cruz (a80564)

Adriana Meireles (a82582)

6 de Outubro de 2019

Conteúdo

Capítulo 1

Introdução

No âmbito da unidade curricular de **Tecnologia de Segurança** foi realizado o Trabalho Prático Nº1 no qual pretendemos apresentar a identificação padrão de vulnerabilidades e exposições publicamente conhecidas, assim como a sua importância nas atividades relacionadas com a segurança de sistemas informáticos.

Capítulo 2

Perguntas

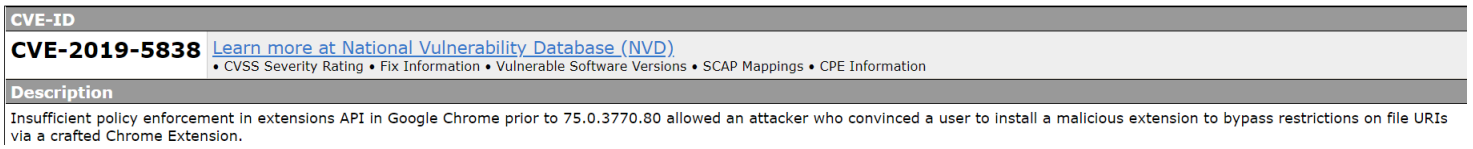
2.1 Pergunta 5.1

As três aplicações típicas usadas no nosso computador são:

- Google Chrome
- Skype
- Spotify

⇒ **Chrome**

A aplicação insuficiente de políticas nas extensões API do Google Chrome permitiu que um atacante convencesse um utilizador a instalar uma extensão maligna para ignorar restrições nos arquivos URIs através de uma extensão do Chrome criada.


CVE-ID

CVE-2019-5838 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Insufficient policy enforcement in extensions API in Google Chrome prior to 75.0.3770.80 allowed an attacker who convinced a user to install a malicious extension to bypass restrictions on file URIs via a crafted Chrome Extension.

Figura 2.1: Vulnerabilidade 1-Chrome

URI: é uma cadeia de caracteres compacta usada para identificar um recurso na Internet.

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 4.3 MEDIUM
Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N (V3.0 legend)
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): None
Integrity (I): Low
Availability (A): None

CVSS v2.0 Severity and Metrics:
Base Score: 4.3 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.6

Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): None
Integrity (I): Partial
Availability (A): None
Additional Information:
Victim must voluntarily interact with attack mechanism
Allows unauthorized modification

Figura 2.2: Impacto da Vulnerabilidade 1-Chrome

O problema do ciclo de vida do objeto em V8 no Google Chrome permitia que um atacante remoto explorasse potencialmente a corrupção da pilha através de uma página HTML criada.

CVE-ID

CVE-2019-5831 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Object lifecycle issue in V8 in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

Figura 2.3: Vulnerabilidade 2-Chrome

Impact

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 (V3.0 legend)
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

CVSS v2.0 Severity and Metrics:
Base Score: 6.8 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 8.6

Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Victim must voluntarily interact with attack mechanism
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

Figura 2.4: Impacto da Vulnerabilidade 2-Chrome

⇒ **Skype**

Existe uma vulnerabilidade de falsificação quando um servidor do Skype *Business 2015* não limpa adequadamente uma solicitação particularmente criada.

CVE-ID

CVE-2019-0624 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A spoofing vulnerability exists when a Skype for Business 2015 server does not properly sanitize a specially crafted request, aka "Skype for Business 2015 Spoofing Vulnerability." This affects Skype.

Figura 2.5: Vulnerabilidade 1-Skype

Impact

CVSS v3.0 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 (V3.0 legend)
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

CVSS v2.0 Severity and Metrics:

Base Score: 3.5 LOW
Vector: (AV:N/AC:M/Au:S/C:N/I:P/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 6.8

Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): Single
Confidentiality (C): None
Integrity (I): Partial
Availability (A): None
Additional Information:
Victim must voluntarily interact with attack mechanism
Allows unauthorized modification

Figura 2.6: Impacto da Vulnerabilidade 1-Skype

Existe uma vulnerabilidade de execução de código remoto no Skype *for Business* quando o software falha na limpeza de conteúdo especialmente criado, também conhecida como "Vulnerabilidade de execução remota de código do Skype for Business".

CVE-ID

CVE-2011-1717 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Skype for Android stores sensitive user data without encryption in sqlite3 databases that have weak permissions, which allows local applications to read user IDs, contacts, phone numbers, date of birth, instant message logs, and other private information.

Figura 2.7: Vulnerabilidade 2-Skype

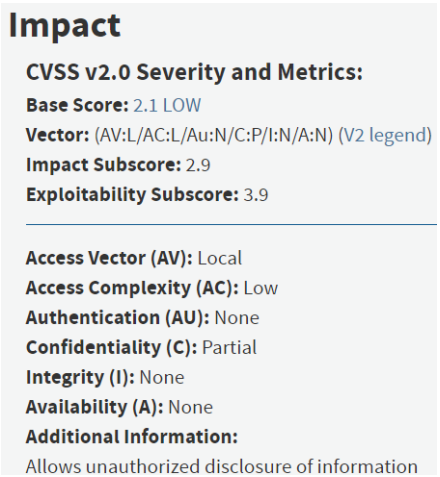


Figura 2.8: Impacto da Vulnerabilidade 2-Skype

⇒ **Spotify**

Para explorar esta vulnerabilidade a interação do utilizador é necessária pois deve visitar uma página maligna. Devido à falta de validação pelo utilizador antes da execução de uma chamada ao sistema vai permitir ao atacante executar o código no contexto do processo corrente.

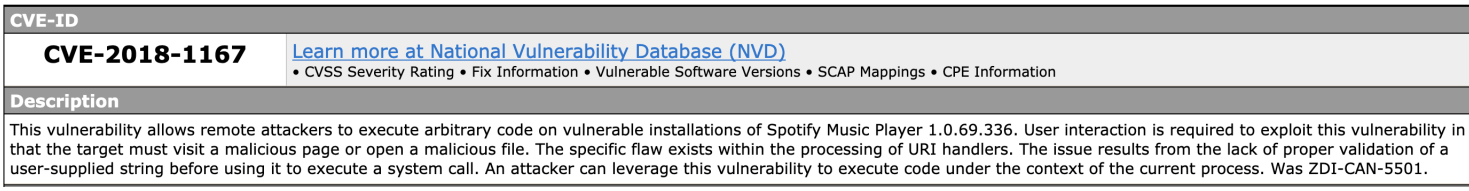
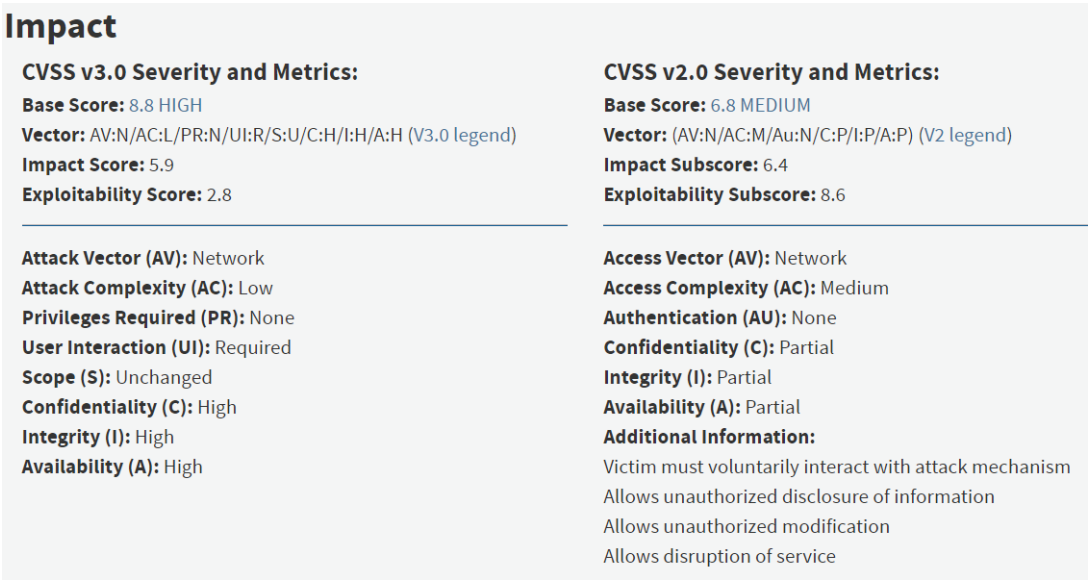


Figura 2.9: Vulnerabilidade-Spotify



Impact

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 (V3.0 legend)
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

CVSS v2.0 Severity and Metrics:

Base Score: 6.8 MEDIUM
Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 8.6

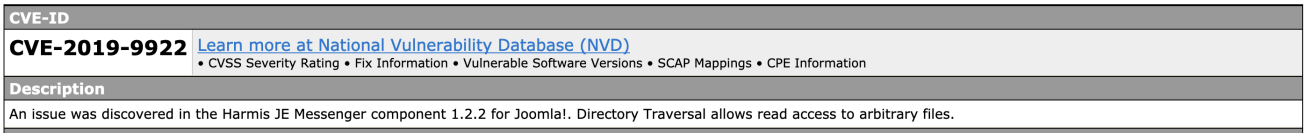
Access Vector (AV): Network
Access Complexity (AC): Medium
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Victim must voluntarily interact with attack mechanism
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

Figura 2.10: Impacto da Vulnerabilidade-Spotify

2.2 Pergunta 5.2

⇒ **Joomla**

Foi descoberto um problema na componente Harmis JE Messenger 1.2.2. O Directory Traversal permite acesso de leitura a arquivos arbitrários.



CVE-ID	
CVE-2019-9922	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. Directory Traversal allows read access to arbitrary files.	

Figura 2.11: Vulnerabilidade 1- Joomla

Impact

CVSS v3.0 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 (V3.0 legend)
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

CVSS v2.0 Severity and Metrics:
Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (V2 legend)
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 2.12: impacto Vulnerabilidade 1- Joomla

Foi descoberto um problema na componente Harmis JE Messenger 1.2.2 para Joomla ! É possível executar uma ação no contexto da conta de outro utilizador.

CVE-ID

CVE-2019-9920 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. It is possible to perform an action within the context of the account of another user.

Figura 2.13: Vulnerabilidade 2- Joomla

Impact

CVSS v3.0 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 (V3.0 legend)
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

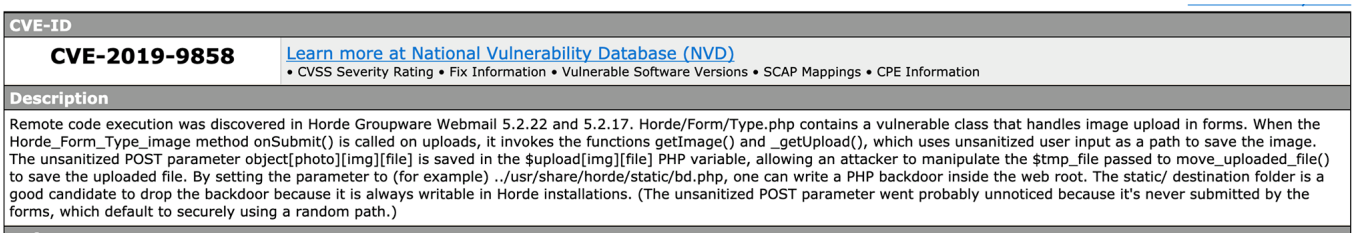
CVSS v2.0 Severity and Metrics:
Base Score: 6.5 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 8.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

Figura 2.14: Impacto da Vulnerabilidade 2 - Joomla

⇒ **PHP**

A execução remota de código foi descoberta no Horde Groupware Webmail 5.2.22 e 5.2.17. Horde / Form / Type.php contém uma classe vulnerável que lida com o upload de imagens em formulários. Quando o método dos uploads é chamado, ele invoca as funções getImage () e getUpload (), que usa entrada não autorizada do utilizador como um caminho para guardar a imagem. Configurando o parâmetro pode escrever-se um backdoor PHP dentro da raiz da web. A pasta destino é um bom candidato para descartar o backdoor, pois é sempre gravável nas instalações do Horde.



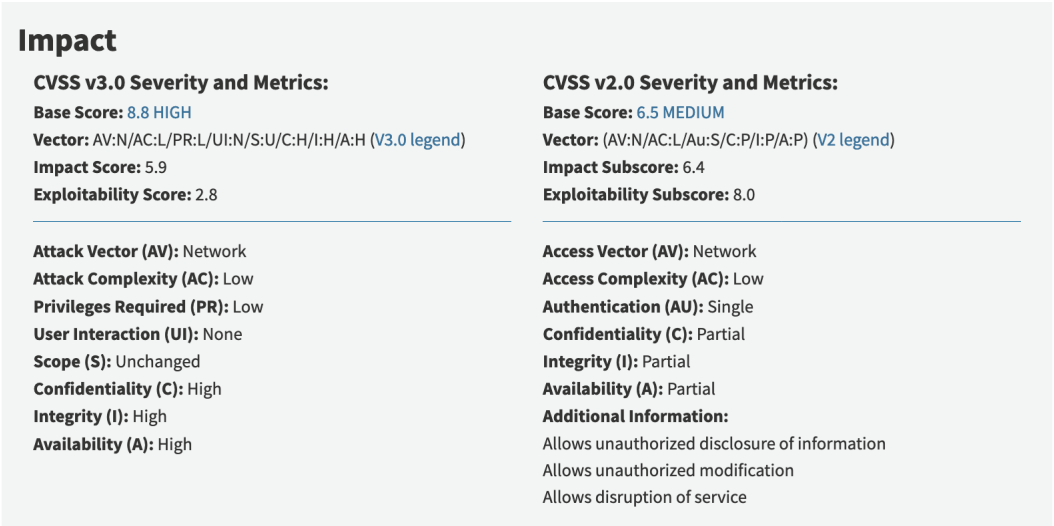
CVE-ID

CVE-2019-9858 — Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Remote code execution was discovered in Horde Groupware Webmail 5.2.22 and 5.2.17. Horde/Form/Type.php contains a vulnerable class that handles image upload in forms. When the Horde_Form_Type_image method onSubmit() is called on uploads, it invokes the functions getImage() and _getUpload(), which uses unsanitized user input as a path to save the image. The unsanitized POST parameter object[photo][img][file] is saved in the $upload[img][file] PHP variable, allowing an attacker to manipulate the $tmp_file passed to move_uploaded_file() to save the uploaded file. By setting the parameter to (for example) ../usr/share/horde/static/bd.php, one can write a PHP backdoor inside the web root. The static/ destination folder is a good candidate to drop the backdoor because it is always writable in Horde installations. (The unsanitized POST parameter went probably unnoticed because it's never submitted by the forms, which default to securely using a random path.)

Figura 2.15: vulnerabilidade 1- PHP



Impact

CVSS v3.0 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 (V3.0 legend)
Impact Score: 5.9
Exploitability Score: 2.8

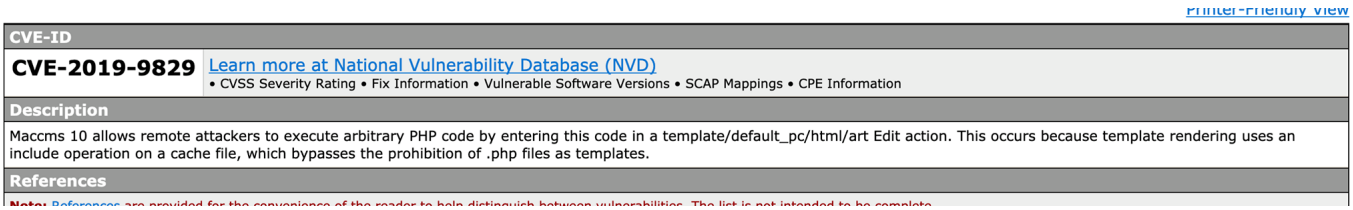
Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:
Base Score: 6.5 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 8.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

Figura 2.16: Impacto da vulnerabilidade 1- PHP

O Maccms 10 permite que atacantes remotos executem código PHP arbitrário inserindo esse código numa ação de edição. Isso ocorre porque a interpretação do modelo usa uma operação de inclusão num arquivo em cache, que ignora a proibição de arquivos .php como modelos.



Printer-Friendly View

CVE-ID

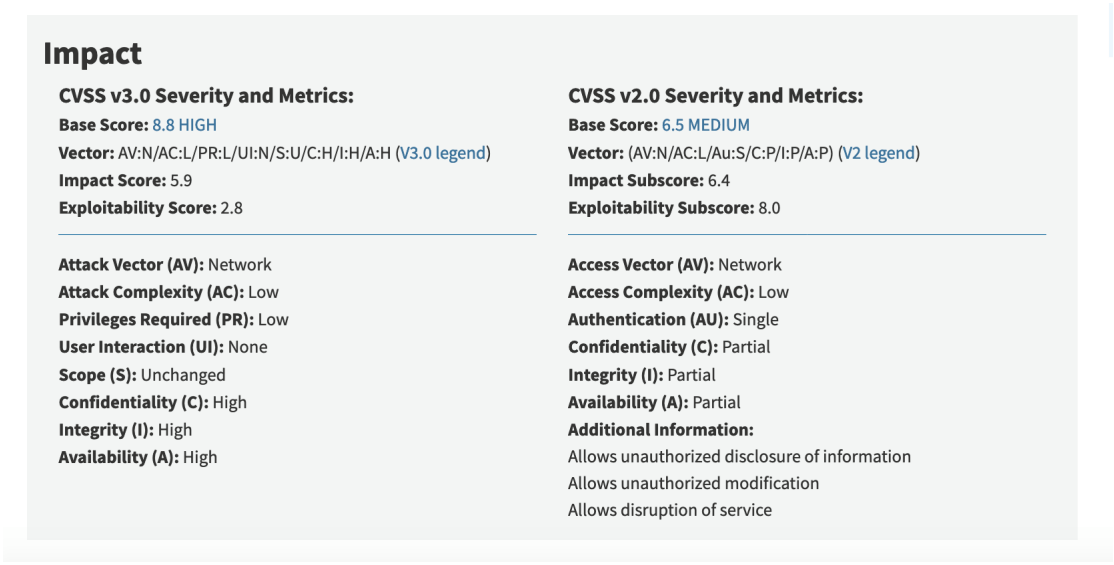
CVE-2019-9829 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Maccms 10 allows remote attackers to execute arbitrary PHP code by entering this code in a template/default_pc/html/art Edit action. This occurs because template rendering uses an include operation on a cache file, which bypasses the prohibition of .php files as templates.

References

Figura 2.17: vulnerabilidade 2- PHP



Impact

CVSS v3.0 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 (V3.0 legend)
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

CVSS v2.0 Severity and Metrics:
Base Score: 6.5 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 8.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service

Figura 2.18: Impacto da vulnerabilidade 2- PHP

2.3 Pergunta 5.3

Heartbleed bug é considerado uma falha grave na biblioteca de software criptográfico open source que é o OpenSSL. Através desta falha de segurança é possível a um atacante aceder a informação protegida pelos protocolos TLS e DTLS. Isto é possível graças à existência da extensão *Heartbeat* que mantém a ligação entre cliente e servidor ativa e permite a obtenção de 64KB de informação a cada "batimento cardıaco".

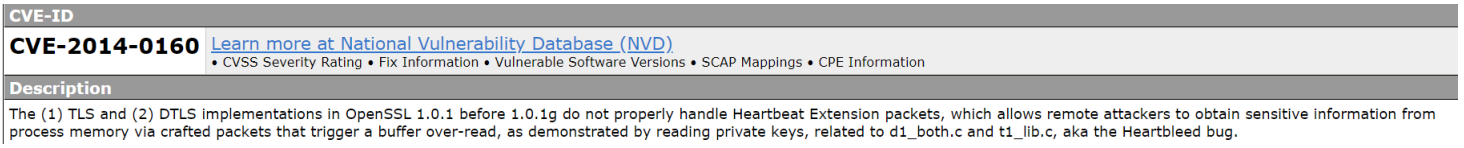


Figura 2.19: Vulnerabilidade OpenSSL

TLS: é um protocolo de segurança responsável por garantir a proteção sobre uma rede de computadores.
DTLS: é um protocolo de comunicação projetado para proteger a privacidade dos dados e impedir a adulteração.

⇒ **Versões afetadas**

Todas as versões do OpenSSL do 1.0.1 até ao 1.0.1f foram afetadas. A 07-04-2014 foi lançada a versão 1.0.1g responsável por corrigir o erro.

⇒ **Exploits existentes**

Foram detetados 4 exploits.

Figura 2.20: Exploits registados para esta falha

⇒ **Vetores de Ataque**

Para além do próprio SSL, exitem outros vetores de ataque tais como:

- **Poodle:** Com o aparecimento do protocolo TLS 1.2 POODLE (Padding Oracle On Downgraded Legacy Encryption) juntamente com a versão 3.0 de SSL é possível que os atacantes forcem a ligação a atingir uma versão menos segura de si mesmo até conseguirem desencriptar cookies enviadas pela mesma ligação SSL.
- **RC4:** é usado um algoritmo denominado RC4. Sendo este um algoritmo criptográfico simétrico, que não é considerado dos melhores algoritmos visto que pode haver aplicações a converter-se em sistemas muito inseguros. No entanto é suportado por diversos browsers e servidores. Assim, foi descoberta uma vulnerabilidade de 13 anos sobre este algoritmo que permitia a atacantes o acesso a credenciais e muitas outras informações durante uma conexão SSL.
- **Beast:** O BEAST explora uma vulnerabilidade no cipher block chaining (CBC) no protocolo TLS v1.0 que foi descoberto em 2002. Como é usado em determinadas configurações como,por exemplo,Microsoft Windows e Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera e outros produtos, o CBC é utilizado para criptografar os dados. Quando esta vulnerabilidade é explorada, permite a realização de ataques do tipo man-in-the-middle.

⇒ **Impacto**

Uma exploração bem-sucedida pode "despejar"informações particularmente sensíveis como, por exemplo, passwords.

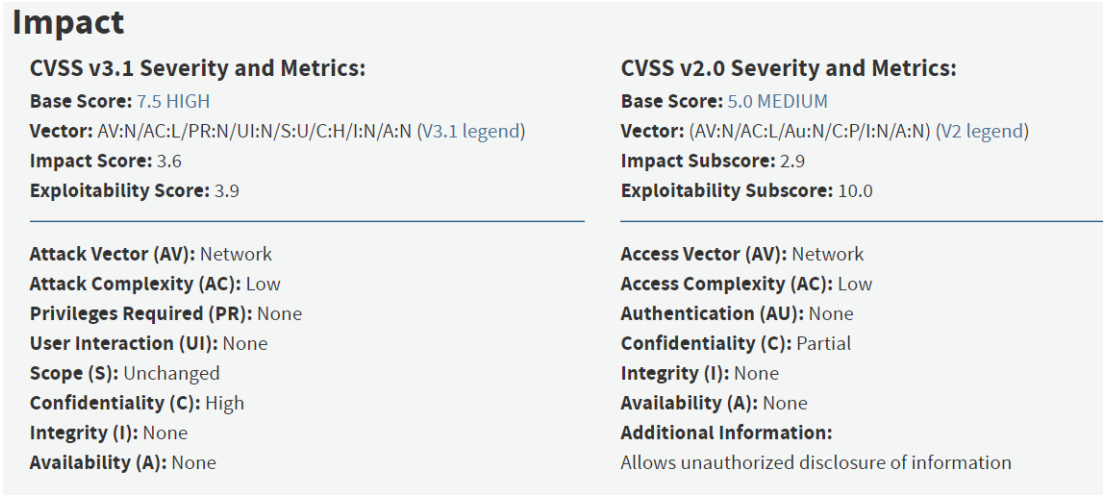


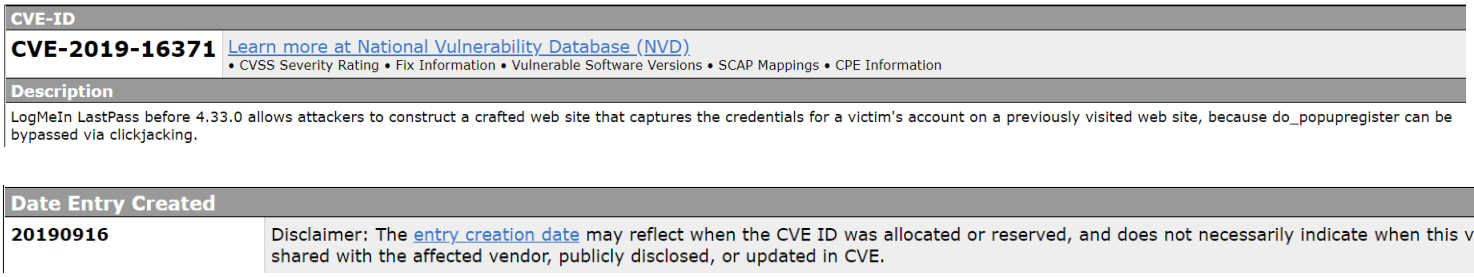
Figura 2.21: Impacto da Vulnerabilidade OpenSSL

⇒ **Soluções**

A principal solução passa por atualizar os servidores com a versão mais recente do OpenSSL(1.0.1g ou mais recente). Outra solução poderia ser pedir aos utilizadores para modificarem as suas passwords.

2.4 Pergunta 5.4

A versão do *LastPass* anterior à 4.33.0 permite aos atacantes construir um site que se apodera das credenciais da conta da vítima a partir de um site visitado anteriormente. Para funcionar, o ataque dependia de "clickjacking",ou seja, a vítima teria que clicar em uma área especificada pela página.



CVE-ID	
CVE-2019-16371	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
LogMeIn LastPass before 4.33.0 allows attackers to construct a crafted web site that captures the credentials for a victim's account on a previously visited web site, because do_popupregister can be bypassed via clickjacking.

Date Entry Created	
20190916	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this v shared with the affected vendor, publicly disclosed, or updated in CVE.

Figura 2.22: Vulnerabilidade LastPass

2.5 Pergunta 5.5

A Mozilla Foundation divulga informações sobre vulnerabilidades as quais os seus produtos foram expostos através do seu Security Advisories. A companhia disponibilizou uma atualização do seu browser, i.e., Firefox ESR 68.1. Assim, iremos apresentar três vulnerabilidades.

Mozilla Foundation Security Advisory 2019-26

Security vulnerabilities fixed in Firefox ESR 68.1

Announced September 3, 2019

Impact critical

Products Firefox ESR

Fixed in Firefox ESR 68.1

⇒ **Malicious code execution through command line parameters**

Os parâmetros da linha de comando relacionados ao log não são limpos adequadamente quando o Firefox é iniciado por outro programa. Isso pode ser usado para gravar um arquivo de log num local arbitrário, como a pasta 'Inicialização' do Windows'.

CVE-2019-11751: Malicious code execution through command line parameters

Reporter Ping Fan (Zetta) Ke of VXRL working with iDefense Labs

Impact critical

Description

Logging-related command line parameters are not properly sanitized when Firefox is launched by another program, such as when a user clicks on malicious links in a chat application. This can be used to write a log file to an arbitrary location such as the Windows 'Startup' folder.
Note: this issue only affects Firefox on Windows operating systems.

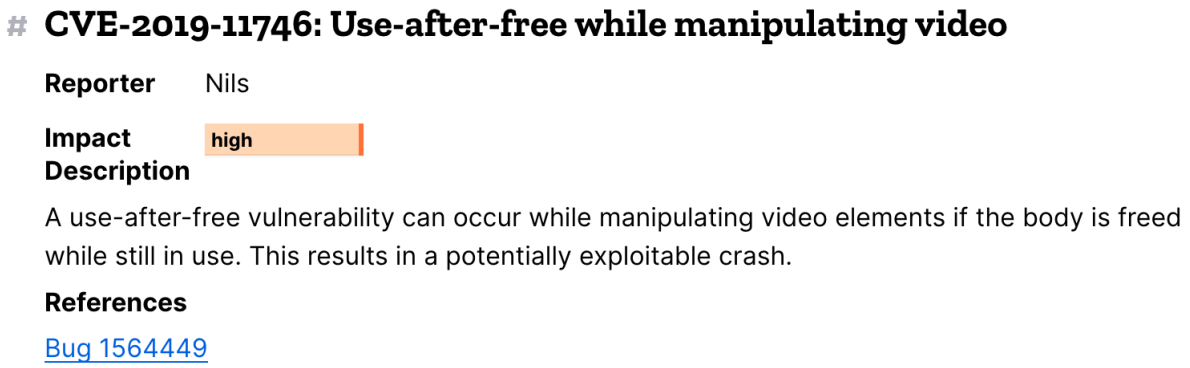
References

Bug 1572838

Figura 2.23: Vulnerabilidade 1- Firefox ESR 68.1

⇒ **Use-after-free while manipulating video**

Uma vulnerabilidade de uso after-free pode ocorrer ao manipular elementos de um vídeo se o "corpo"for libertado enquanto ainda estiver em uso. Isso resulta numa falha potencialmente explorável.



CVE-2019-11746: Use-after-free while manipulating video

Reporter Nils

Impact high

Description

A use-after-free vulnerability can occur while manipulating video elements if the body is freed while still in use. This results in a potentially exploitable crash.

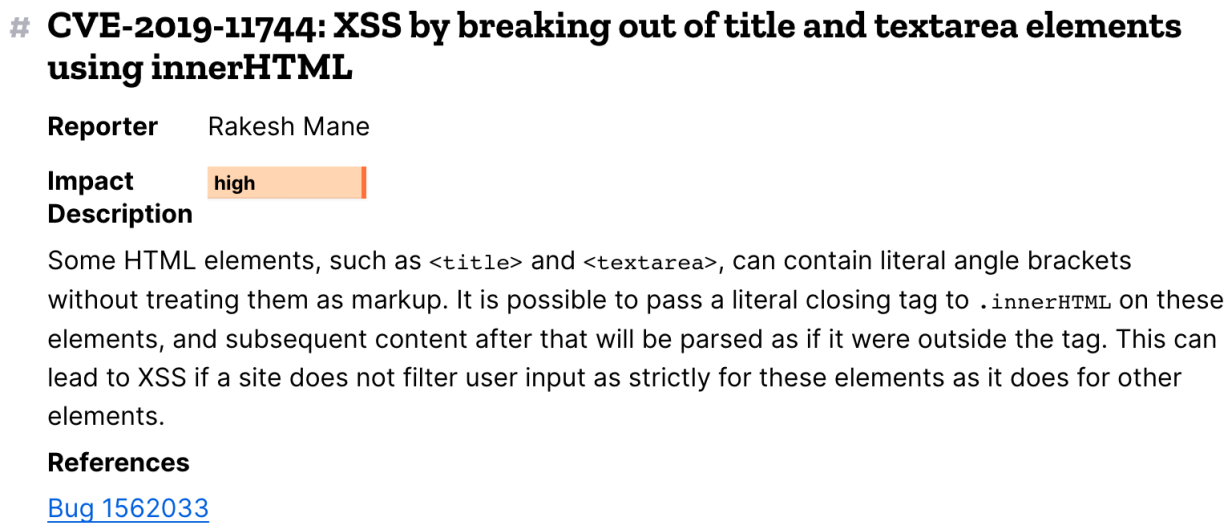
References

Bug 1564449

Figura 2.24: Vulnerabilidade 2- Firefox ESR 68.1

⇒ **XSS by breaking out of title and textarea elements using innerHTML**

Alguns elementos HTML, como o título e a zona do texto, podem conter chavetas angulares sem tratá-los como marcação. É possível passar uma tag de fecho para .innerHTML nesses elementos, e o conteúdo subsequente será analisado como se estivesse fora da tag. Isso pode levar a que o XSS de um site comece a não filtrar a entrada do utilizador tão estritamente para esses elementos quanto para outros.



CVE-2019-11744: XSS by breaking out of title and textarea elements using innerHTML

Reporter Rakesh Mane

Impact high

Description

Some HTML elements, such as `<title>` and `<textarea>`, can contain literal angle brackets without treating them as markup. It is possible to pass a literal closing tag to `.innerHTML` on these elements, and subsequent content after that will be parsed as if it were outside the tag. This can lead to XSS if a site does not filter user input as strictly for these elements as it does for other elements.

References

Bug 1562033

Figura 2.25: Vulnerabilidade 3- Firefox ESR 68.1

Capítulo 3

Conclusão

Com a realização deste trabalho ficámos a conhecer novas ferramentas como ,por exemplo, *CVE* e *Exploit Database* que nos permitiu compreender mais sobre vulnerabilidades de programas.

A realização deste trabalho e deixou-nos motivadas para trabalhos seguintes desta Unidade Curricular.