Segurança de Sistemas Informáticos

TPC1

a85954 Luís Ribeiro

1 Exercicío 1

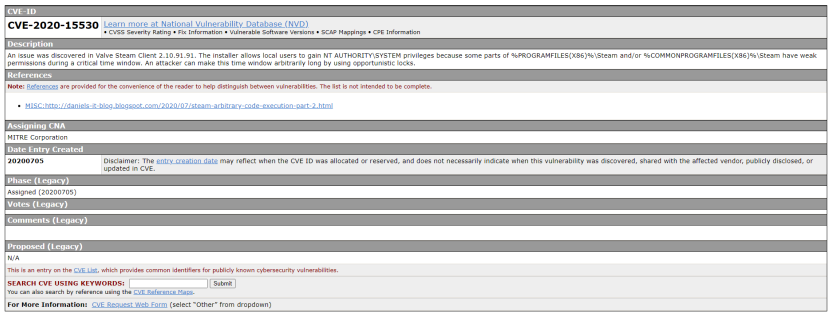
As aplicações escolhidas foram as seguintes: Steam, TeamSpeak3 e Opera

1.1 Steam

Vulnerabilidade: CVE-2020-15530

Descrição: Em Julho de 2020, foi exposto uma vulnerabilidade/problema na versão 2.10.91.91 da Valve Steam Client. O instalador permitia que os "local users"obtivessem privilégios de acesso (NT AUTHORITY SYSTEM privileges)por causa da existência de permissões não protegidas ("weak premissions") durante periodos de tempo curtos.

Exploração: Estes períodos podiam ser prolongados com o uso de locks.



CVE-ID

CVE-2020-15530 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 Valve Steam Client 2.10.91.91. The installer allows local users to gain NT AUTHORITY\SYSTEM privileges because some parts of %PROGRAMFILES(X86)%\Steam and/or %COMMONPROGRAMFILES(X86)%\Steam have weak permissions during a critical time window. An attacker can make this time window arbitrarily long by using opportunistic locks.

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:http://daniels-it-blog.blogspot.com/2020/07/steam-arbitrary-code-execution-part-2.html

Assigning CNA

MITRE Corporation

Date Entry Created

20200705 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 (20200705)

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: 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

1.1.1 Análise das métricas do CVSS

CVSS Base Score: 7.8
Exploitability Subscore: 1.8

- Attack Vector: Local
- Attack Complexity: Low
- Privileges Required: Low
- User Interaction: None
- Scope: Unchanged

Impact Subscore: 5.9

- Confidentiality Impact: High
- Integraty Impack: High
- Availability Impact: High

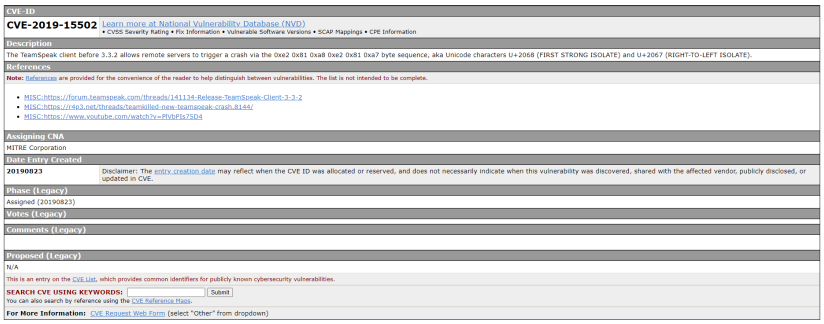
Figura 2: CVSS 3.x Severity and Metrics

1.2 TeamSpeak3

Vulnerabilidade: CVE-2019-15502

Descrição: Em Agosto de 2019, foi exposto uma vulnerabilidade na versão 3.3.2 do Team Speak Client, identificado por CVE-2019-15502.

Exploração: Através de uma sequência de bytes (0xe2 0x81 0xa8 0xe2 0x81 0xa7) os "remote servers"podiam bloquear/crashar o cliente.



CVE ID

CVE-2019-15502 Learn more at National Vulnerability Database (NVD)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The TeamSpeak client before 3.3.2 allows remote servers to trigger a crash via the 0xe2 0x81 0xa8 0xe2 0x81 0xa7 byte sequence, aka Unicode characters U+2068 (FIRST STRONG ISOLATE) and U+2067 (RIGHT-TO-LEFT ISOLATE).

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://forum.teamspeak.com/threads/141134-Release-TeamSpeak-Client-3-3-2
- MISC:https://r4p3.net/threads/teamkilled-new-teamspeak-crash.8144/
- MISC:https://www.youtube.com/watch?v=PVbPIs75D4

Assigning CNA

MITRE Corporation

Date Entry Created

20190823 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 (20190823)

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: 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

1.2.1 Análise das métricas do CVSS

CVSS Base Score: 7.5
Exploitability Subscore: 3.9

- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: Low
- User Interaction: None
- Scope: Unchanged

Impact Subscore: 3.6

- Confidentiality Impact: None
- Integraty Impack: None
- Availability Impact: High

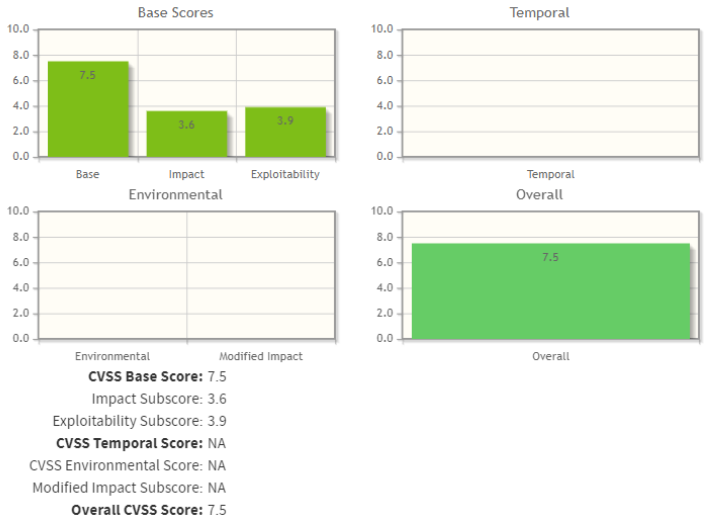


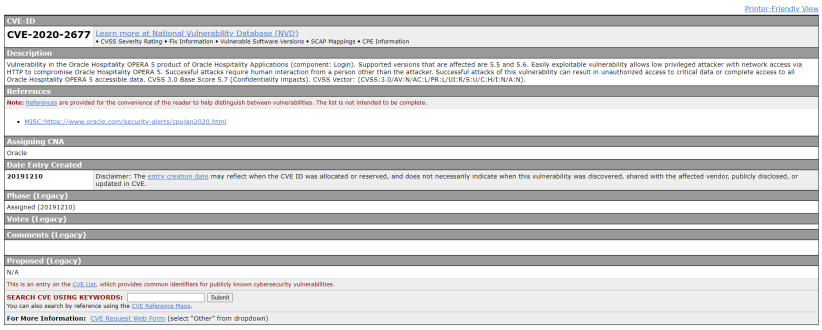
Figura 4: CVSS 3.x Severity and Metrics

1.3 Opera

Vulnerabilidade: CVE-2020-2677

Descrição: Em Fevereiro de 2020, foi exposto uma vulnerabilidade nas versões 5.5 e 5.6 do Oracle Hospitality OPERA 5, identificado por CVE-2020-2677.

Exploração:"Attackers"com privilégios baixos podiam comprometer o Oracle Hospitality via HTTP. Este vulnerabilidade permitia acessos não autorizados a dados críticos e o acesso completo aos dados do Oracle Hospitality.


Printer-Friendly View

CVE ID

CVE-2020-2677 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Vulnerability in the Oracle Hospitality OPERA 5 product of Oracle Hospitality Applications (component: Login). Supported versions that are affected are 5.5 and 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 accessible data. CVSS 3.0 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N).

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://www.oracle.com/security-alerts/cpujan2020.html

Assigning CNA

Oracle

Date Entry Created

20191210 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 (20191210)

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: 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

1.3.1 Análise das métricas do CVSS

CVSS Base Score: 5.7
Exploitability Subscore: 2.1

- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: Low
- User Interaction: Required
- Scope: Unchanged

Impact Subscore: 3.6

- Confidentiality Impact: High
- Integraty Impack: None
- Availability Impact: None

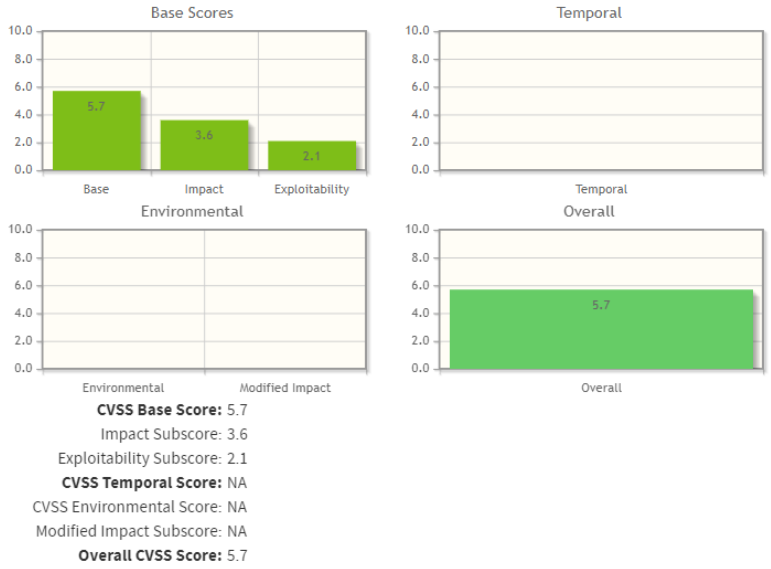


Figura 6: CVSS 3.x Severity and Metrics

2 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.

Esta vulnerabilidade permitia o "roubo"de informação protegida, em condições normais, pela criptografia do SSL/TLS usada para proteger a Internet. SSL/-TLS fornece segurança e privacidade na comunicação nas aplicações dentro da Internet.

O bug "Heartbleed"permitia que alguém lesse facilmente a memória dos sistemas protegidos pelas versões do OpenSSL afetadas. Isto comprometia os Service Providers e a informação dos seus utilizadores. Assim, era possível o roubo de informação e o disfarce, isto é, o uso de dados de outro utilizador.

As versões entre o OpenSSL 1.0.1 through 1.0.1f (inclusive) são vulneráveis.

São possíveis encontrar 4 exploits no *Explit Database*, alguns deles são derivações de outros.

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 7: Exploits encontrados

As métricas do CVSS calculadas foram as seguintes:

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

Figura 8: Vector CVSS

Enquanto as versões vulneráveis do OpenSSL estiverem em uso, o bug pode

ser explorado. No entanto, Fixed OpenSSL foi lançado e implementado. Os Service Providers e os utilizadores têm que instalar o "fix"quando se torna disponível.

A equipa do OpenSSL corrigiu e lançou a versão 1.0.1g já corrigida. Se não for possível usar esta versão, é possível recompilar o OpenSSL sem o "handshake"habitual através da opção de compilação *-DOPENSSL_NO_HEARTBEATS*.

3 Exercício 3

Em 02 de setembro de 2020, a companhia disponibilizou uma atualização (Firefox for Android 80). Esta versão resolve uma série de vulnerabilidades listadas no relatório MFSA 2020-39. Das vulnerabilidades, escolhi as seguintes:

- **CVE-2020-15671:** Passwords podiam ser guardadas dentro do teclado do telemóvel
- **CVE-2020-12400:** P-384 e P-521 vulneráveis ataques de canal lateral
- **CVE-2020-15670:** *Memory safety bugs*

3.1 CVE-2020-15671: Passwords podiam ser guardadas dentro do teclado do telemóvel

Descrição: Quando se introduzia a *password* dentro de certas condições, podia acontecer um erro de perceção do *input field*, onde a *password* escrita/introduzida era guardada no dicionário do teclado.

Versões afetadas: Esta vulnerabilidade afeta as versões do Firefox abaixo da 80.

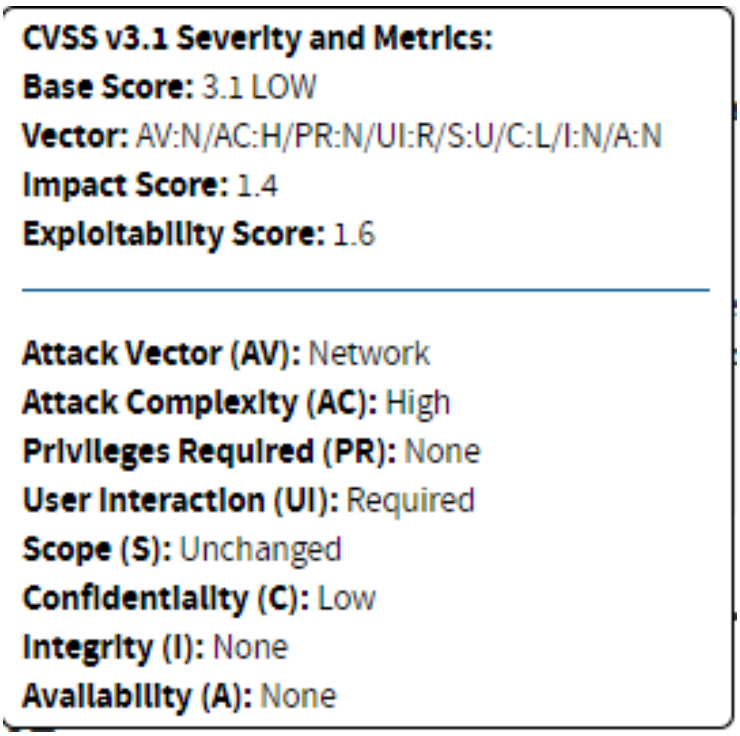


Figura 9: CVSS 3.x Metrics

3.2 CVE-2020-12400: P-384 e P-521 vulneráveis ataques de canal lateral

Descrição: Quando ocurria uma certa conversão de coordenadas, a inversão modular não era realizada em tempo constante, resultando num possível ataque temporizado (Timing-Based attack).

Versões afetadas: Esta vulnerabilidade afeta as versões do Firefox abaixo da 80, e as versões para mobile abaixo da 80.

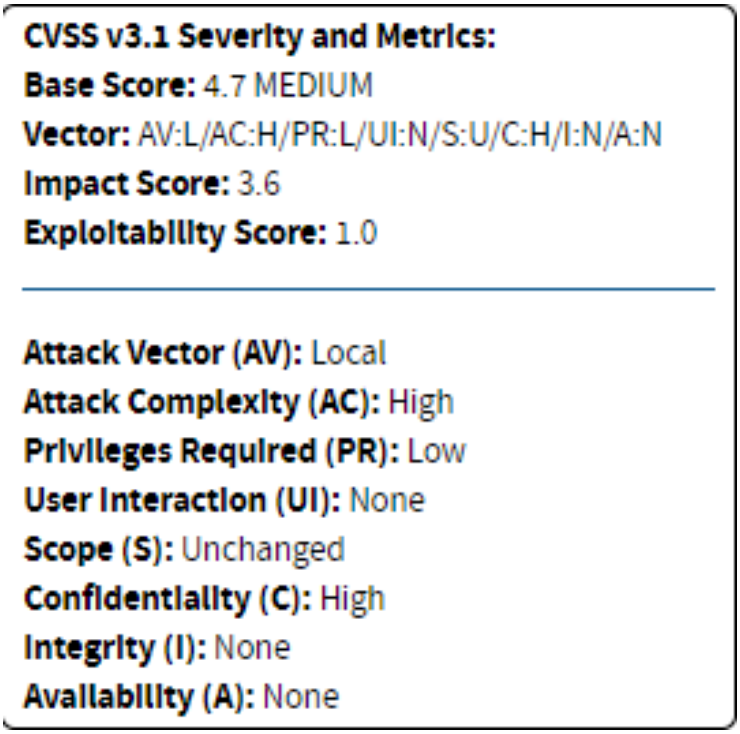


Figura 10: CVSS 3.x Metrics

3.3 CVE-2020-15670: *Memory safety bugs*

Descrição: 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 externo.

Versões afetadas: Esta vulnerabilidade afeta as versões do Firefox abaixo da 80, versões para mobile do Firefox abaixo da 80, as versões do Thunderbird abaixo da 78.2 e versões abaixo da Firefox ESR 78.2.

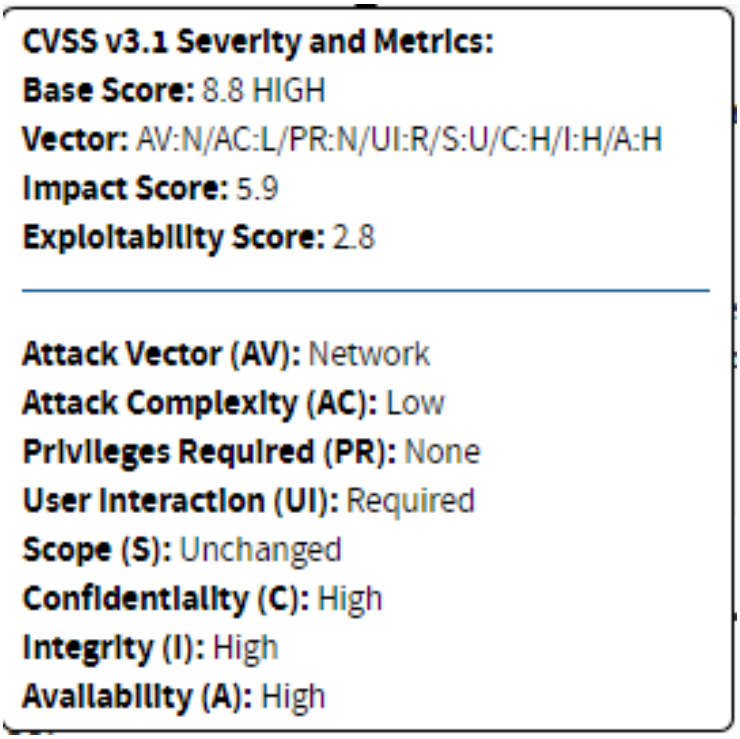


Figura 11: CVSS 3.x Metrics

4 Exercício 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 em Cookies sem a sua validação

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.