****

**Segurança de Sistemas Informáticos**

**Ficha de Exercicios 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.

|  |  |
| --- | --- |
| Uma imagem com pessoa, parede, interior, pose  Descrição gerada automaticamente | **Uma imagem com pessoa, parede, homem, interior  Descrição gerada automaticamente** |
| A91697 - Luís Filipe Fernandes Vilas | A91671 - João Manuel Novais da Silva |
|  |  |
|  |  |
|  | |
|  | |

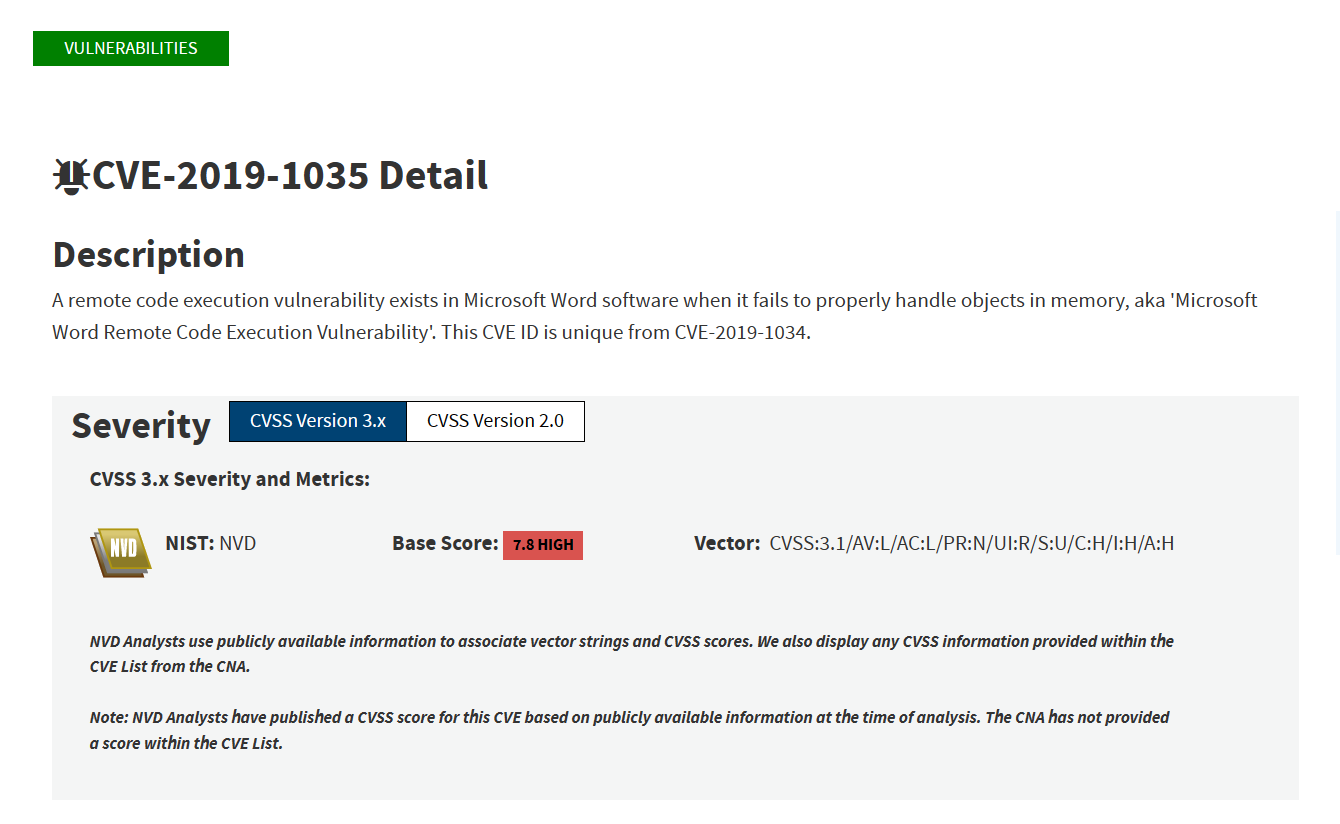
**Prazo de submissão: 23:59 de 28/03/2023**

**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 vitima.



# Google Chrome

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

Uma imagem com texto

Descrição gerada automaticamente

# AnyDesk

CVE-2020-13160

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 victima.

Uma imagem com texto

Descrição gerada automaticamente

**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.

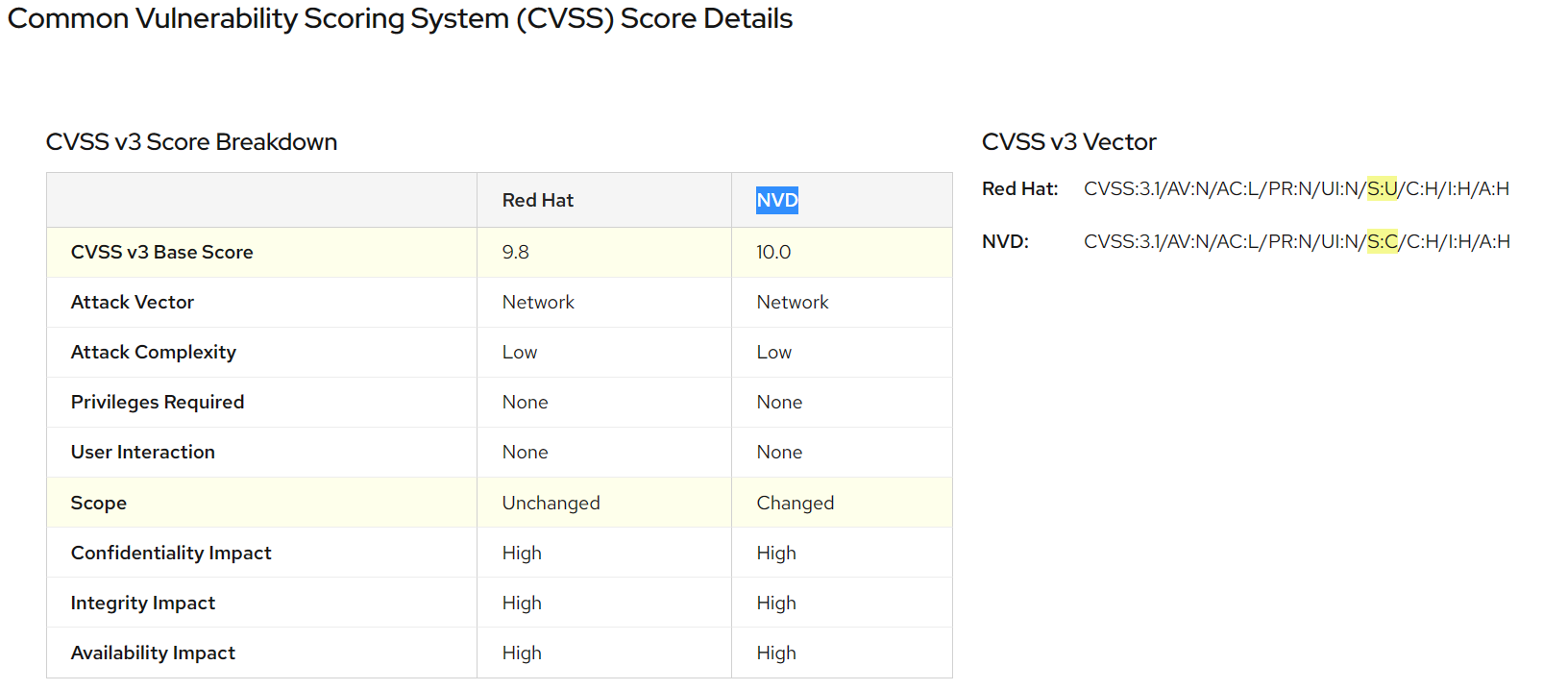
O Vector de ataque desta falha era a Rede e o mesmo tinha pouca complexidade.

Exitem 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:

Uma imagem com texto

Descrição gerada automaticamente



Uma imagem com texto

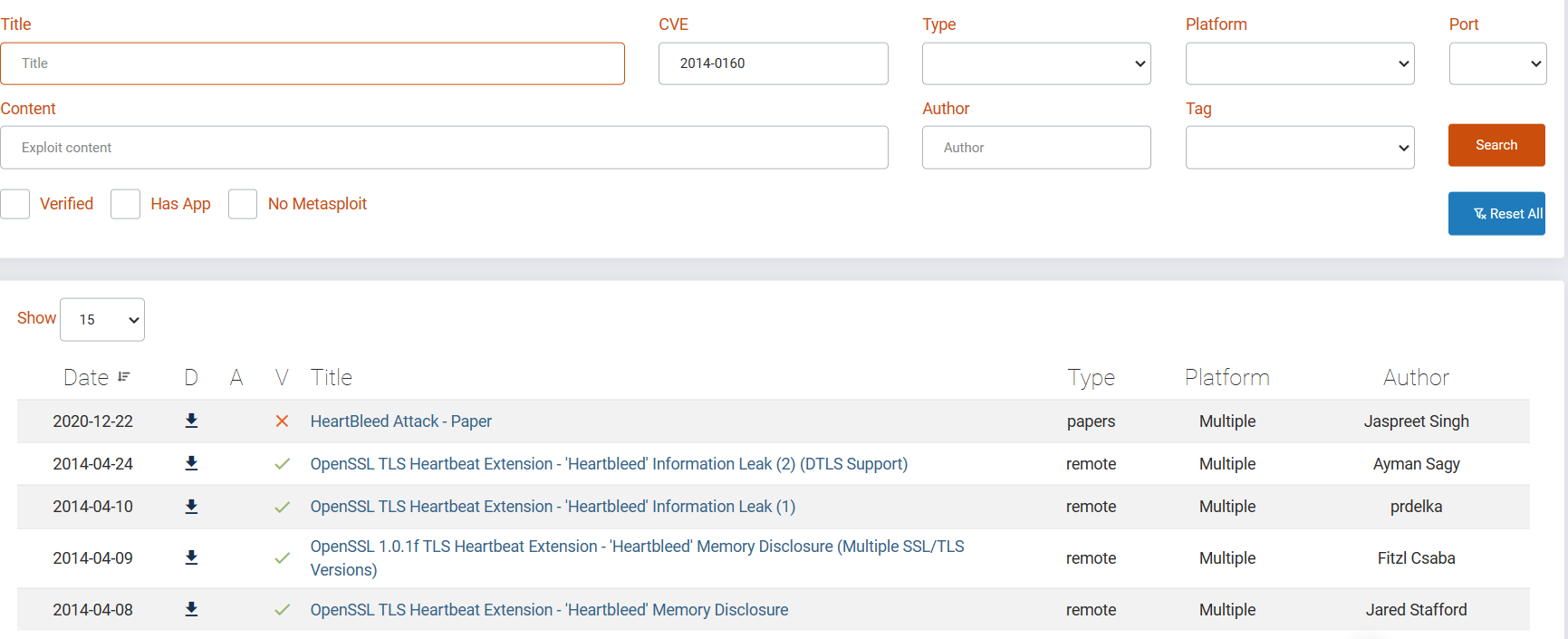
Descrição gerada automaticamente

**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 vitima, 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:



Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

**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.](https://www.mozilla.org/en-US/security/advisories/mfsa2023-10/) Descreva *detalhadamente* duas vulnerabilidades listadas neste relatório e identificada como de possível alto impacto (i.e., *high)*.

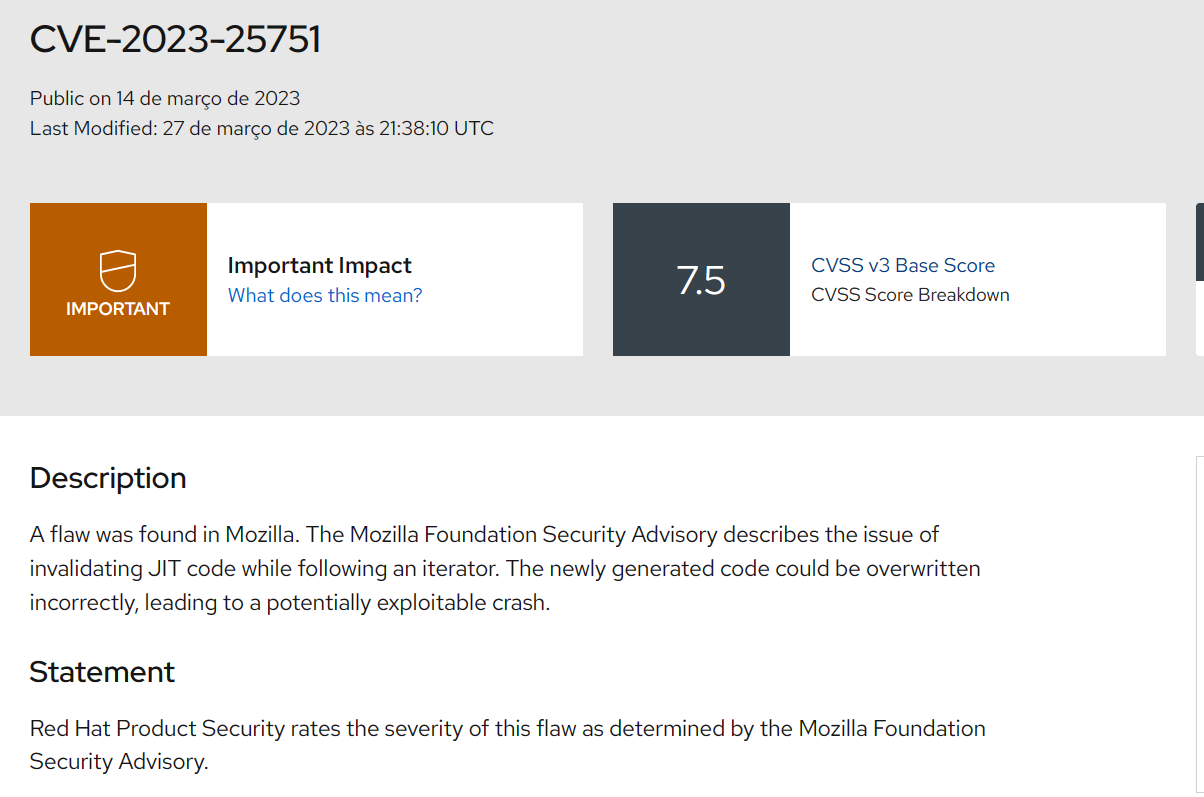
# Resposta

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-2023-28176

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



**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.