Información Actualizada 27/01/2022: Vulnerabilidad crítica en Apache Log4j 2

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, informa del estado en el que se encuentra la vulnerabilidad que afecta a la librería Apache Log4j 2.

Como se ha alertado durante los últimos días, se ha hecho pública una vulnerabilidad que afecta a la librería de registro de Java Apache Log4j 2, herramienta desarrollada por *Apache Foundation* que ayuda a los desarrolladores de software a escribir mensajes de registro, cuyo propósito es dejar constancia de una determinada transacción en tiempo de ejecución, además, *Log4j* permite filtrar los mensajes en función de su importancia.

La vulnerabilidad, a la que se le ha asignado el CVE-2021-44228 y se ha denominado *Log4Shell*, es del tipo de ejecución de código remoto no autenticado, permitiendo a un atacante, tomar el control del equipo mediante el manejo adecuado de la entrada al registro de logs.

Debido a la gravedad de esta vulnerabilidad, la Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones ruega encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a la vulnerabilidad.

Recursos Afectados (*Actualizado 21/12/2021*):

La vulnerabilidad afecta a las siguientes versiones:

- **Apache Log4 desde la versión 2.0 hasta la 2.16.**

Posibles Vectores de Entrada

La vulnerabilidad puede ser explotada fácilmente en múltiples aplicaciones y servidores, una recopilación de aplicaciones comerciales afectadas es la siguiente https://github.com/NCSC-NL/log4shell/blob/main/software/README.md

El exploit puede ser usado en campos propios de las aplicaciones de cada organismo usando los parámetros de comunicaciones o los datos de los formularios de la aplicación.

Se debe prestar especial atención a los siguientes parámetros de entrada de las aplicaciones con conexión a Internet:

- X-Api-Version
- User-Agent
- Referer
- X-Druid-Comment
- Origin
- Location
- X-Forwarded-For
- Cookie

- X-Requested-With
- X-Forwarded-Host
- Accept

Recomendaciones (*Actualizadas 27/01/2022*)

Detección de la vulnerabilidad

Paso 1. Para revisar **si se está usando la versión vulnerable** de *log4j*:

- Windows (PowerShell):

  ```
  gci 'C:\' -rec -force -include *.jar -ea 0 | foreach {select-string "JndiLookup.class" $_} | select -exp Path
  ```

- Linux:

  ```
  find / 2>/dev/null -regex ".*.jar" -type f | xargs -I{} grep JndiLookup.class "{}"
  ```

- Para otras formas alternativas de localización, consulte las siguientes indicaciones que ofrece CCN-CERT en su artículo "CCN-CERT AL 09/21 Actualización vulnerabilidad en Apache Log4j 2 (14/12/2021)"

> ***Si estos comandos arrojan resultados, se debe comprobar si la versión es vulnerable.***

Paso 2. Independientemente de lo indicado en el punto anterior, se debe **verificar** que el equipo está protegido con el **EPP corporativo**, dispone de las **últimas firmas publicadas y** tiene el **módulo IPS instalado y habilitado**.

> ***Recordamos que el producto está disponible tanto para Windows como para Linux***

Paso 3. Es **altamente recomendable instalar** el **EDR de Crowdstrike**, cuyo procedimiento se encuentra a continuación:

- **Verificar incompatibilidad de versiones NO soportadas:**

  All other Windows OSes are unsupported, including but not limited to:

  All pre-GA versions/builds of Windows – Windows Insider Preview, beta, etc – unless specifically stated in a Release Note. Including but not limited to:

  Windows 11 Preview Builds

  Windows Server 2022 Preview Builds

Windows 7 hosts without a CrowdStrike Extended Support subscription as of January 14, 2021 [https://supportportal.crowdstrike.com/s/article/SupportAnnouncement-Falcon-Sensor-Support-Policy-for-Windows-7-SP1-and-Windows-Server-2008-R2-SP1] .

Windows Server 2008 R2 hosts without a CrowdStrike Extended Support subscription as of January 14, 2021 [https://supportportal.crowdstrike.com/s/article/Support-Announcement-Falcon-Sensor-Support-Policy-for-Windows-7-SP1-and-Windows-Server-2008-R2-SP1] .

Windows Server 2008 (non-R2), which is based on the Vista kernel

Windows Server Core, all versions other than 2016 and 2019

Windows 10 64-bit v1511, aka Threshold 2

Windows 10 64-bit v1703, aka Redstone 2 ("RS2")

Windows 10 64-bit v1709, aka Redstone 3 ("RS3")

Windows 10 64-bit v1803, aka Redstone 4 ("RS4")

Windows 10 64-bit v1903, aka 19H1

All 32-bit versions of Windows 10 not listed above

All 32-bit versions of Windows 8.1

All versions of Windows 8

Container-based Windows OS solutions, including but not limited to Docker, are not currently supported.

Windows Embedded Standard 7 is unsupported. This version is independent from Windows 7 Embedded POS Ready, which is the only Embedded version we

do support.

- **Verificar** que en el equipo donde se vaya a desplegar el EDR tiene acceso a las siguientes urls y debe aparecer como resultado la palabra "**ok**":

EU-1
ts01-lanner-lion.cloudsink.net
lfodown01-lanner-lion.cloudsink.net

- **Para Windows.**
  - ***En Servidores***: Descargar el siguiente instalador y seguir las instrucciones que se indican en el fichero Readme-Server.txt

    Instalador Crowdstrike_Servidores.7z

  - ***En PCs***. Descargar el siguiente instalador y seguir las instrucciones que se indican en el fichero Readme-PC.txt

    Instalador Crowdstrike_PCs.7z

NOTA: Importante verificar los requisitos de comunicaciones antes de proceder a la instalación.

Procedimiento completo: Falcon Sensor for Windows Deployment _ Documentation _ Support _ Falcon.pdf.

- **Para Linux.**
  - Verificar compatibilidad del Kernel en el procedimiento completo.
  - Instalar con el comando apropiado según distribución (ver procedimiento completo). La instalación requiere privilegios de sudo.
  - Establecer el CID que figura en el punto anterior.
  - Establecer opciones de proxy si se requieren
  - Establecer Grouping_Tags. Se recomienda usar la cadena “SERVERS_***PROVINCIA***” Sustituyendo provincia por la que corresponda.

Version Linux	Ejecutable sensor EDR
Debian	falcon-sensor_6.33.0-13003_amd64.deb
RHEL_CentOS_Oracle6	falcon-sensor-6.33.0-13003.el6.x86_64.rpm
RHEL_CentOS_Oracle7	falcon-sensor-6.33.0-13003.el7.x86_64.rpm
RHEL_CentOS_Oracle8	falcon-sensor-6.33.0-13003.el8.x86_64.rpm
Ubuntu	falcon-sensor_6.33.0-13003_amd64.deb

NOTA: Importante verificar los requisitos de comunicaciones antes de proceder a la instalación.

Procedimiento completo: Falcon Sensor for Linux Deployment _ Documentation _ Support _ Falcon.pdf.

Mitigación

1º. Solución a la vulnerabilidad:

Apache ha lanzado la **versión Log4j-2.17.0** para abordar esta vulnerabilidad. Para más información sobre cómo instalar las actualizaciones y las distintas extensiones se dispone del siguiente enlace:

- Download Apache Log4j 2.

2º. Workaround de la vulnerabilidad:

En caso de no poder efectuar la actualización a las versiones indicadas anteriormente, debe realizar los siguientes pasos:

1. Como medidas de mitigación, en versiones anteriores (>=2.10), este comportamiento puede resolverse estableciendo la propiedad del sistema:

```
log4j2.formatMsgNoLookups = true
```

2. o eliminando la clase JndiLookup del classpath, como, por ejemplo:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

3. Java 8u121 protege contra esta RCE al establecer por defecto:

```
com.sun.jndi.rmi.object.trustURLCodebase = false
com.sun.jndi.cosnaming.object.trustURLCodebase = false
```

NOTA: Adicionalmente, aplicar las medidas de mitigación descritas en los avisos de fabricantes afectados.

3º. Incluir IOCs (Indicadores de Compromiso) en proxies y firewalls provinciales

La lista de IOC se está ampliando según avanzan las investigaciones. Les sugerimos varios enlaces para actualizar listados de IPs que realizan escaneos activos e intentos de explotación de la vulnerabilidad:

- https://community.riskiq.com/article/57abbfcf/indicators
- https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html

Actualmente desde la USTIC estamos trabajando en un sistema de implementación automática de IOC para el ámbito de la seguridad corporativa en distintas líneas de servicios de seguridad (proxies, firewalls, EDR,...)

Los proxies **SQUID** son los primeros elementos de seguridad en los que se están pilotando esta solución, mediante una servicio de descarga diaria de los IOC del repositorio de Andalucia-CERT e integración en listas de denegación de Ip y dominios.

Este repositorio de Andalucia-CERT , a su vez, proviene de los análisis de la cibertinteligencia de la herramienta **RE YES** (CCN-CERT).

Los **IOC que recomienda CCN-CERT** , que corresponden a indicadores de explotación de la vulnerabilidad, ya están incluidos en REYES, por lo que **se recomienda que se traten de manera automática** a través de la ejecución del script preparado para tal efecto.

El **script de configuración para la descarga e incorporación de los IOCs automática** es el siguiente: ScriptIOCautomatic.sh . En este script hay que sustituir <*password_ftp*> por la clave. Contactar con ustic.stic.sspa@juntadeandalucia.es para el envío de dichas credenciales.

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indicando en el *Asunto: [Compromiso log4j]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es. Les seguiremos informando.

Gracias por su atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud
