# BOLETÍN DE ALERTA

**Boletín Nro.**: 2021-42

**Fecha de publicación**: 29/12/2021

**Tema**: Nueva vulnerabilidad RCE en Apache Log4j.

**Software afectado:**

- **Apache Log4j en todas las versiones desde 2.0-alpha7 a 2.17.0, excepto 2.3.2 y 2.12.4.**

**Descripción:**

Apache ha publicado una actualización de seguridad para abordar la CVE-2021-44832, una vulnerabilidad de severidad media con una puntuación temporal de 6.6, la cual es vulnerable a un ataque de ejecución remota de código (RCE), en donde un atacante con permiso para modificar el archivo de configuración de registro puede construir una configuración maliciosa utilizando un Appender JDBC con una fuente de datos que hace referencia a un URI JNDI que puede ejecutar código remoto.

**JDBC Appender**

Un Appender JDBC escribe eventos de registro en una tabla de base de datos relacional utilizando JDBC estándar. Este se puede configurar para obtener conexiones JDBC utilizando un origen de datos JNDI o un método de fábrica personalizado.

Se debe tener presente que el Appender JDBC configurado con un DataSource requiere soporte JNDI, por lo que a partir de la versión 2.17.1 este appender no funcionará a menos que **log4j2.enableJndiJdbc=true** esté configurado como una propiedad del sistema o variable de entorno.

Adicionalmente a esta última actualización, los encargados del mantenimiento del proyecto de Apache Log4j han logrado mitigar un total de 4 vulnerabilidades mencionadas a continuación:

- CVE-2021-44228 (Puntuación de 10.0). Vulnerabilidad de ejecución remota de código (RCE). Mitigado en la versión 2.15.0.

- CVE-2021-45046 (Puntuación de 9.0). Vulnerabilidad de divulgación de información y ejecución remota de código (RCE). Mitigado en la versión 2.16.0.
- CVE-2021-45105 (Puntuación de 7.5). Vulnerabilidad de denegación de servicio (DoS). Mitigado en la versión 2.17.0.
- CVE-2021-4104 (Puntuación de 8.1). Vulnerabilidad de escalamiento de privilegios en la versión 1.2 de Log4j. No mitigado debido a que la versión 1.x ya no posee soporte y se debe actualizar a la última versión disponible de Log4j 2.x.

**Impacto:**

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

**Detección:**

Para comprobar si su aplicación es vulnerable puede utilizar la herramienta de verificación proveída por CISA.

**Solución:**

Se recomienda actualizar Apache Log4j a las versiones 2.17.1 (Java 8), 2.12.4 (Java 7) y 2.3.2 (Java 6) que pueden ser descargadas del siguiente enlace:

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

**Información adicional:**

- https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44832
- https://thehackernews.com/2021/12/new-apache-log4j-update-released-to.html
- https://www.bleepingcomputer.com/news/security/log4j-2171-out-now-fixes-new-remote-code-execution-bug/
- https://vuldb.com/?id.189422
- https://nvd.nist.gov/vuln/detail/CVE-2021-44832
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228

- https://nvd.nist.gov/vuln/detail/CVE-2021-45105
- https://nvd.nist.gov/vuln/detail/CVE-2021-4104