



> _Log4Shell

CVE-2021-44228 con una puntuación CVSS de 10.

CVE-2021-44228 - Log4j RCE

[Details](#) [Content](#) [Version History](#)

This pack handles Apache Log4j RCE CVE-2021-44228, a 0-day exploit in the popular Java logging library log4j2.

This pack is part of the [Rapid Breach Response](#) pack.

Critical RCE Vulnerability: log4j - CVE-2021-44228 refers to a 0-day exploit in the popular Java logging library log4j2.

On Dec. 9, 2021, a remote code execution (RCE) vulnerability in Apache log4j 2 was identified being exploited in the wild. Public proof of concept (PoC) code was released and subsequent investigation revealed that exploitation was incredibly easy to perform.

This pack will provide you with a first response kit which includes:

- Hunting
- Remediation
- Mitigations

PUBLISHER
Cortex XSOAR

INFO

Certification ● Certified [Read more](#)

Supported By Cortex XSOAR

Created December 11, 2021

Last Release December 13, 2021

[Hunting](#) [Incident Response](#)

¿QUÉ DEBES HACER EN CORTEX?

La Unidad 42 está monitoreando activamente el tráfico anormal a través de nuestros dispositivos y soluciones en la nube. Palo Alto Networks proporciona protección contra la explotación de esta vulnerabilidad:

XDR



Los clientes que **ejecutan agentes Linux** y el contenido 290-78377 están protegidos de una cadena de explotación completa mediante el módulo de protección **Java Deserialization Exploit**.

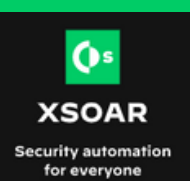
Otros clientes están protegidos contra varias cargas útiles observadas derivadas de **CVE-2021-44228** a través de **Behavioral Threat Protection (BTP)**.

XDR PRO

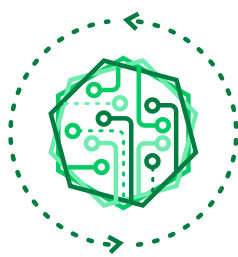


Quienes cuentan con Cortex XDR Pro y que utilicen **Analytics tendrán detectadas actividades posteriores** a la explotación relacionadas con esta vulnerabilidad.

XSOAR



Los clientes de **Cortex XSOAR** pueden aprovechar el paquete "**CVE-2021-44228 - Log4j RCE**" para detectar y mitigar automáticamente la vulnerabilidad.



¡MANTÉNTE ALERTA!



Mantente al tanto de las alerta y comunicados

Palo Alto Networks continuará monitoreando la situación y nos mantendrá actualizados en estos links con cualquier hallazgo o información nueva.

<https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-protection-modules.html>

https://xsoar.pan.dev/marketplace/details/CVE_2021_44228

<https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/>

<https://security.paloaltonetworks.com/CVE-2021-44228>

<https://register.paloaltonetworks.com/unit42threatbriefingapache>

¿NECESITAS AYUDA?

Habla con nosotros →