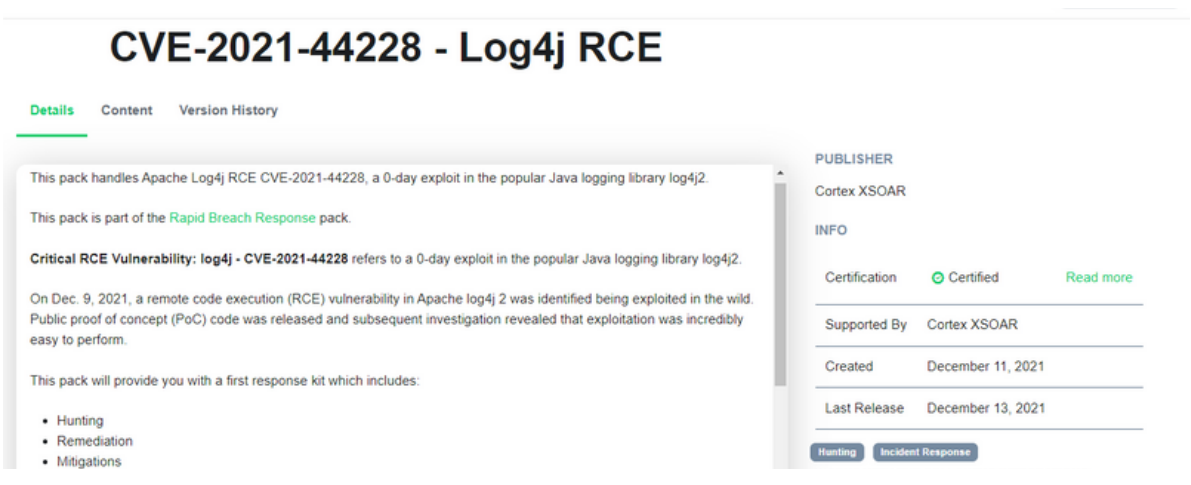
>_Log4Shell

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



¿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 post**eriores 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

Grupo Smartekh | paloalto NETWORKS | paloalto NextWave Platinum Innovator | paloalto Certified Professional Services Partner | CYBERFORCE

Más información en www.smartekh.com