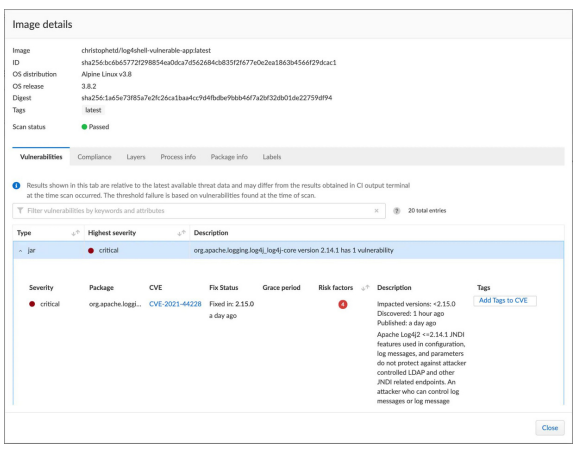
paloalto | UNIT 42

>_Log4Shell

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



¿QUÉ DEBES HACER EN PRISMA CLOUD?

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:

Los agentes de **Prisma Cloud Compute Defender** pueden detectar si algún proyecto de integración continua (CI), imagen de contenedor o sistema host mantiene un paquete Log4j vulnerable o un archivo JAR con una versión igual o anterior a 2.14.1.

Además, las reglas de seguridad de API y aplicaciones web (WAAS) se pueden utilizar para detectar y bloquear cargas útiles de explotación

RECOMENDACIONES

- ✓ Aunque recomendamos aplicar los parches lo antes posible, una mitigación temporal para quienes ejecutan **Log4j 2 versiones 2.10** o posteriores es establecer la propiedad del sistema **log4j2.formatMsgNoLookupso** la variable de entorno **LOG4J_FORMAT_MSG_NO_LOOKUPS**en true.
- ✓ Alternativamente, en versiones anteriores a 2.10, elimine la **JndiLookupclase** de la **classpath zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class** como se recomienda en la guía oficial de Apache.
- ✓ Hay un parche virtual disponible para los usuarios de **Prisma Cloud Web Application y API Security (WAAS) Enterprise** y los usuarios de Compute que ejecutan la última versión de la consola (21.08.525, Actualización 2).
- ✓ Recomendamos a los usuarios que **habiliten este parche virtual en Prevent** en sus aplicaciones existentes abriéndolas, navegando a reglas personalizadas y seleccionando el parche virtual.

¡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://www.paloaltonetworks.com/blog/prisma-cloud/log-4-shell-vulnerability/

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