>_Log4Shell

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

CVE-2021-44228 Informativo: Impacto de la vulnerabilidad de Log4j CVE-2021-44228

Vector de ataque **RED**
Complejidad de ataque **BAJA**
Privilegios requeridos **NINGUNO**
Interacción del usuario **NINGUNO**
Alcance **CAMBIADO**
Impacto en la confidencialidad **NINGUNO**
Impacto en la integridad **NINGUNO**
Impacto en la disponibilidad **NINGUNO**

NVD JSON
Publicado **2021-12-10**
Actualizado **2021-12-14**
Referencia
Descubierto **externamente**

¿QUÉ DEBES HACER EN TU FIREWALL?

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 firewalls de próxima generación con una **Suscripción de Seguridad de Prevención de amenazas pueden bloquear automáticamente** las sesiones relacionadas con esta vulnerabilidad mediante ID de amenazas:

NGFW

- **91991** (lanzado inicialmente con la actualización de contenido de Aplicaciones y Amenazas versión 8498 y mejorado con la versión 8499). Además, la infraestructura de los atacantes se supervisa y bloquea continuamente.
- **91994 y 91995** (lanzados con la versión 8500 de contenido de amenazas de aplicaciones).

RECOMENDACIONES

✓ Para los usuarios que confían en **Snort o Suricata**, se han publicado las siguientes reglas : 2034647, 2034648, 2034648, 2034649, 2034650, 2034651, 2034652

✓ Los clientes de aplicaciones que aprovechan Apache log4j deben actualizar a la versión más reciente.

Dado que se descubrió que se había omitido el parche original, en aras de implementar tantas protecciones contra esta vulnerabilidad como sea posible, también se recomiendan las siguientes mitigaciones:

✓ Deshabilita el tráfico saliente sospechoso, como **LDAP y RMI e**n el servidor en PANW Firewall.

- Deshabilite la búsqueda JNDI.
  - Configurar **log4j2.formatMsgNoLookups = true**
  - Elimine el archivo **JndiLookup en log4j-core** y reinicie el servicio.
- Deshabilitar JNDI
  - Configurar **spring.jndi.ignore = true**

¡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://register.paloaltonetworks.com/unit42threatbriefingapache

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

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

¿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