Logjam: los intentos de ataque de Log4j continúan globalmente

- *Direcciones IP en China y Rusia, asociadas a la botnet minera Kinsing, dominan como la principal fuente de intentos de ataque.*

CIUDAD DE MÉXICO. 22 de diciembre de 2021.- Desde que se reveló la primera vulnerabilidad en la herramienta de registro Log4j de Apache el 10 de diciembre, se lanzaron tres conjuntos de parches y actualizaciones a la biblioteca de Java a medida que se descubrieron vulnerabilidades adicionales.

Esta rápida respuesta ha dejado a los desarrolladores de software y a las organizaciones de todo el mundo luchando por evaluar y mitigar su exposición con un entorno que cambia casi a diario. Mientras tanto, hemos visto que los intentos de explotar la vulnerabilidad continúan sin parar.

A medida que transcurre la primera semana desde la vulnerabilidad inicial, en SophosLabs hemos continuado rastreando los intentos contra las redes para explotar Log4Shell, incluyendo tanto análisis benignos realizados por investigadores de seguridad, como actividad maliciosa.

Lo cierto es que ante esos datos no hemos visto una reducción significativa en los intentos de exploits desde que alcanzaron su punto máximo el 15 de diciembre. Además hemos detectado que provienen de una infraestructura distribuida globalmente.

Por ejemplo, en algunos casos, un intento de ataque proviene de una dirección IP en una región geográfica, intentando redirigir al usuario a una URL integrada para Log4j que se conecta a servidores que se encuentran en otros lugares.

¿Quién está haciendo esto?

Si bien no podemos distinguir la intención de cada intento de vulneración, hemos encontrado hasta ahora que la gran mayoría proviene de direcciones IP en Rusia y China. Esto no incluye el tráfico que oculta su origen mediante el uso de redes privadas virtuales; una cantidad de tráfico estadísticamente significativa se enruta a través del punto de salida de NordVPN en Panamá, por ejemplo.

Debido a la forma en que funcionan los exploits de Log4j, al solicitar "búsquedas" en servidores remotos y protocolos compatibles con Java Name and Directory Interface (JNDI), las solicitudes se pueden dirigir a una ubicación diferente a la fuente del exploit. Por ejemplo, una solicitud enrutada a través del punto de salida de Panamá de NordVPN utilizó una redirección a una URL en Kenia. En general, casi dos tercios de estas solicitudes tenían una URL para infraestructura en India y más del 40% tenía URL dirigidas a infraestructura en los Estados Unidos.

Hay que mencionar que los números aún no son del todo claros ya que, por ejemplo, más del 7% de los intentos de explotación se dirigieron a un dominio de la herramienta Interactsh, pero esta ha sido utilizada tanto por investigadores como por actores malintencionados.

Es decir, es difícil separar los intentos benignos de los ataques reales como ocurre con gran parte del resto del tráfico que estamos detectando y bloqueando actualmente. Pero está claro que los intentos de explotación maliciosa siguen siendo la mayoría de este tráfico.

Mitigación y protección

Cuando se lanzó el primer parche para Log4j, el equipo de Apache ofreció una serie de soluciones para evitar la explotación. Pero todas estas correcciones resultaron ser discutibles a medida que se descubrieron rutas de vulnerabilidad adicionales.

La única forma segura de protegerse contra la explotación, ya sea para obtener la ejecución remota de código o para causar la denegación de servicio, es actualizar el software para usar las versiones "seguras" actuales de Log4j.

Varias agencias gubernamentales de seguridad informática mantienen una lista de productos comerciales vulnerables, incluida la Administración de Seguridad de Infraestructura y Ciberseguridad (CISA) de EU. Las organizaciones deben evaluar la vulnerabilidad de su software lo antes posible e implementar actualizaciones cuando sea posible.

En donde las actualizaciones aún no están disponibles, las herramientas de filtrado de red pueden proteger contra un gran porcentaje del tráfico de exploits existente, pero no garantizan la protección contra amenazas emergentes y ataques altamente dirigidos.

###

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/