Log4Shell Hell: anatomía de un 'brote' de exploits en Javascript

- *Una vulnerabilidad en un componente de registro de Java ampliamente utilizado está exponiendo a un número incalculable de organizaciones a posibles ataques de código remoto y robo de información.*

CIUDAD DE MÉXICO. 14 de diciembre de 2021.- El 9 de diciembre, se reveló una grave vulnerabilidad de código remoto en Log4J, un componente de registro muy común entre los desarrolladores de aplicaciones web basadas en el lenguaje de programación Javascript. Esta vulnerabilidad afecta a una amplia gama de servicios y aplicaciones, lo que la hace extremadamente peligrosa e incrementa la necesidad de nuevas actualizaciones para dichos sistemas.

La vulnerabilidad hace posible que cualquier atacante pueda inyectar texto y modificar los parámetros de configuración del servidor que carga el código para el desarrollo de la aplicación; de ese modo, el servidor ejecuta ese código modificado mediante llamadas a la Interfaz de directorio y nombres de Java (JNDI).

Ya habiendo vulnerado JNDI, este interactúa con varios servicios de red, incluido el Protocolo ligero de acceso a directorios (LDAP), el Servicio de nombres de dominio (DNS), la Interfaz remota de Java (RMI) y el Agente de solicitud (CORBA). De ese modo, los entes maliciosos pueden dirigir a los usuarios de esas aplicaciones desde LDAP, DNS y RMI, hacia una URL redirigida a un servidor externo con código modificado.

Sophos identificó diversas operaciones maliciosas de criptomineros que intentan aprovechar la vulnerabilidad, y hay informes de que varias botnets automatizadas (como Mirai, Tsunami y Kinsing) también han comenzado a explotarla.

Es probable que se produzcan rápidamente otros tipos de ataques. Si bien hay pasos que los operadores del servidor pueden tomar para mitigar la vulnerabilidad, la mejor solución es actualizar a la última versión con los parches correspondientes, ya lanzada por Apache en Log4j 2.15.0. Sin embargo, la implementación de una actualización puede no ser tan simple, especialmente si las organizaciones no saben dónde se implementó como componente.

En el pasado, se han encontrado vulnerabilidades de inyección JNDI críticas similares en otros componentes del servidor Java, incluida una en la implementación del Protocolo Inter-ORB de Internet (IIOP) del servidor WebLogic de Oracle (CVE-2020-2551). Pero el uso generalizado de Log4J en software comercial y de código abierto conectado a Internet hace que sea una vulnerabilidad especialmente difícil de rastrear.

Sophos ya ha detectado cientos de miles de intentos de ataque desde el 9 de diciembre, para ejecutar código de forma remota utilizando esta vulnerabilidad, y las búsquedas de registros de

otras organizaciones sugieren que la vulnerabilidad puede haber sido explotada abiertamente durante semanas antes de su exposición pública. Sophos ha detectado principalmente escaneos de la vulnerabilidad, pruebas de explotación e intentos de instalar mineros de criptomonedas. También hemos visto intentos de extraer información, incluidas las claves de Amazon Web Services (AWS) y otros datos privados.

¿Cómo opera?

La falla en Log4J es causada por una característica llamada sustitución de búsqueda de mensajes. Cuando está habilitado (que estaba, de forma predeterminada, antes de la corrección del error), Log4j detectaba cadenas que hacen referencia a recursos JNDI en fuentes de configuración, mensajes de registro y parámetros pasados de las aplicaciones.

Debido a que Log4J no desinfecta las URL pasadas en estas cadenas, un atacante puede crear aplicaciones que usan Log4J haciendo cadenas de sustitución de mensajes para dirigir el tráfico hacia una URL para un servidor malicioso.

En el caso de las aplicaciones web, la cadena podría ser parte de una comunicación HTTP que se registraría, formateada como un comando de sustitución que hace referencia al servidor malicioso.

Entonces, los comandos de búsqueda que usan JNDI dan como resultado que Log4J se comunique con un servidor (local o remoto) para obtener el código Java. En el escenario benigno, este código ayudaría a generar los datos que se pretenden registrar. Pero la esencia de esta vulnerabilidad es que este mismo mecanismo permite la ejecución de código Java remoto, malicioso y no verificado.

Los atacantes emiten solicitudes donde los encabezados HTTP están "rociados" con cadenas maliciosas, construidas para provocar que la aplicación receptora realice la sustitución del mensaje, momento en el que la aplicación activa la vulnerabilidad y carga o ejecuta el código remoto.

SophosLabs ha implementado una serie de escaneos en los sistemas en busca de tráfico que intente aprovechar la vulnerabilidad Log4J. La empresa detectó que durante el fin de semana, el tráfico dirigido a Log4J comenzó a aumentar, y el mayor aumento se produjo el sábado 11 de diciembre por la noche.

La gran mayoría de este tráfico (alrededor del 90%) usaba el protocolo LDAP como objetivo de exploits. Al examinarlo, parte de este tráfico puede haber sido escaneo interno en busca de vulnerabilidades por parte de las organizaciones, pero gran parte parecían ser sondas de sistemas explotables por parte de los atacantes.

Resolver la vulnerabilidad de Log4J requiere una defensa en profundidad. Las organizaciones deben implementar reglas para bloquear el tráfico malicioso de todos los servicios conectados

a Internet, pero la protección a largo plazo requerirá identificar y actualizar instancias de Log4J o mitigar el problema cambiando la configuración. Eso puede requerir cambios de código en productos donde este protocolo está incrustado.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:

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