La Oficina de Seguridad Pública y Seguridad Nacional y la Oficina de Oportunidades para Empresas de Comunicaciones (OCBO) de la Comisión Federal de Comunicaciones le aconseja a la comunidad de pequeñas empresas que tome medidas de seguridad de internet para protegerse de la "vulnerabilidad Log4j de Apache" (“Apache Log4j Vulnerability”)

Los funcionarios de seguridad que trabajan para las agencias gubernamentales federales, incluida la Comisión Federal de Comunicaciones (FCC), tomaron conocimiento recientemente de un defecto serio en un código abierto ampliamente utilizado llamado "Log4j" que consiste en una herramienta de registro de eventos desarrollada en Java. Las agencias ya se encuentran trabajando para mitigar esta vulnerabilidad que conlleva que cientos de millones de dispositivos estén al alcance de ejecuciones remotas de códigos y corran riesgo de *hackeos* o secuestro de datos por parte de grupos criminales. La FCC insta a la comunidad de pequeñas empresas a proteger sus redes informáticas de la vulnerabilidad del *software* Log4j.

¿Qué es la herramienta Log4j?

Los desarrolladores de *software* utilizan la herramienta Log4j para registrar actividades de usuarios y comportamientos de aplicaciones para una revisión posterior. La fundación sin fines de lucro *Apache Software Foundation* distribuye el *software* Log4j de manera gratuita. Log4j es una de las herramientas más utilizadas para la recolección de información en redes informáticas, sitios web y aplicaciones corporativos.

En los siguientes enlaces encontrará una guía de la agencia de seguridad cibernética y seguridad de infraestructura (*Cybersecurity and Infrastructure Security Agency*, CISA, por sus siglas en inglés), una agencia gubernamental federal, donde podrá consultar más información y mantenerse al día sobre las soluciones que se estén desarrollando:

- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- https://www.msspalert.com/cybersecurity-news/log4j-zero-day-vulnerability-cisa-mitigation-patch-guidance/

Si tiene alguna duda o desea obtener una guía más detallada, contáctese con la CISA por teléfono al (888)282-0870 o con el centro de intercambio y análisis de información (Multi-State Information Sharing and Analysis Center, MS-ISAC, por sus siglas en inglés), 24x7 Security Operations Center (centro de operaciones de seguridad, atiende las 24 horas del día, los 7 días de la semana): SOC@cisecurity.org, 1-866-787-4722.

La CISA, mediante el centro de intercambio y análisis de información (MS-ISAC), emitió la siguiente guía sobre la vulnerabilidad Log4j. Según las instrucciones, se recomiendan las siguientes Tácticas, Técnicas y Procedimientos (TTP):

ACCIONES RECOMENDADAS POR LA CISA:

16 de diciembre de 2021, pasos actualizados a seguir en el presente:

1. Escanee todos los *softwares* y sistemas para determinar si existe el archivo .jar de log4j. Vuelva al 30 de noviembre y utilice esta lista de funciones *hash* vulnerables.
2. Utilice el monitor *Huntress* en cada uno de los sistemas para determinar si la funcionalidad de log4j está presente fuera de un archivo .jar fácilmente localizable.
3. Busque cambios de configuración no autorizados en todos los sistemas.
4. Bloquee conexiones salientes en el cortafuegos para todos los servidores afectados.
5. Busque declaraciones públicas de cada proveedor dentro de su red y agréguelos a un rastreador para gestionarlo en las siguientes semanas.

6. Si el proveedor no emitió una declaración pública y es de vital importancia para usted que lo haga, ínstelo a emitirla.

14 de diciembre - RECOMENDACIONES ACTUALIZADAS:

- ***Dado que la iteración del parche 2.15.0 anterior no soluciona completamente el problema de la vulnerabilidad, se recomienda aplicar el último parche (versión 2.16.0) que proporciona Apache luego de realizar las pruebas correspondientes.***
- Ejecutar todos los sistemas y servicios como usuario no privilegiado (usuario sin privilegios de administrador) para disminuir los efectos de un ataque exitoso.
- Aplicar el "principio de mínimo privilegio" (*Principle of Least Privilege*) a todos los sistemas y servicios.

13 de diciembre - RECOMENDACIONES:

- Ejecutar el monitoreo de vulnerabilidad "Log4Shell" ("Log4Shell" Vulnerability Tester) provisto por *Huntress* para detectar si las aplicaciones son vulnerables al CVE-2021-44228 (consulte las referencias para obtener el enlace de *Huntress*).
- Consulte el repositorio de *GitHub* que se encuentra en la sección de referencia para ver todos los Avisos y Boletines de Seguridad (*Security Advisories & Bulletins*) relacionados con el CVE-2021-44228, entre los que se incluyen las aplicaciones afectadas, los números de versiones y los parches asociados que deberían implementarse si su versión se viera afectada.

Si desea obtener más información, contáctese por los siguientes medios:

CISA, (888)282-0870

Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive,
East Greenbush, NY 12061

24/7 Security Operations Center, SOC@cisecurity.org
1-866-787-4722