Log4j, la vulnerabilidad más crítica de la década

Para aquellas personas que no están tan familiarizadas con esta vulnerabilidad, se preguntarán por qué gobiernos e instituciones alrededor del mundo la califican como una de las más complejas de solución en la historia reciente. ¿A qué se debe esta complejidad y qué implicaciones tiene?

El 24 de noviembre, se detectó una de las vulnerabilidades más críticas de la última década en Log4j Shell, una librería de código abierto desarrollada por Apache Foundation y construida sobre el lenguaje Java. Las noticias alrededor del mundo se inundaron de pánico con la vulnerabilidad encontrada en el logging frame work más utilizado del mundo: log4j.

Para aquellas personas que no están tan familiarizadas con esta vulnerabilidad, se preguntarán por qué gobiernos e instituciones alrededor del mundo la califican como una de las más complejas de solución en la historia reciente. ¿A qué se debe esta complejidad y qué implicaciones tiene? ¿Por qué tanto alboroto?.

log4j es un software de código abierto (accesible a todo el público) utilizado por un sinfín de organizaciones, tanto para sus programas corporativos como para sus servicios de gestión en la nube, así como por miles de aplicaciones y páginas web que registran datos. Como lo puedes imaginar, es casi inexistente la aplicación o website que no tenga esta funcionalidad de registro de datos, de ahí la ubicuidad del uso y de la vulnerabilidad de log4j.

Sin embargo, la gravedad de esta vulnerabilidad radica en que la propia librería de logs, utilizada por empresas y aplicaciones, entre otros, para guardar el historial de transacciones, intercambios de paquetes y actualizaciones, con el fin de detectar fallos o amenazas a la hora de solucionar un problema, puede ser una entrada para que ciberdelincuentes tomen control total de los dispositivos comprometidos.

Esta brecha de ciberseguridad recién descubierta permitiría que ciberatacantes puedan ejecutar cualquier software, incluyendo tomar el control total de servidores, conocido como un ataque de ejecución remota de código (RCE, por sus siglas en inglés). Es decir, aquellas plataformas y sitios web que estén comprometidos con esta vulnerabilidad, corren el peligro de ser controladas por ciberatacantes, **obteniendo toda su información e incluso su dinero.**

Miles de profesionales de la ciberseguridad trabajan de manera incansable con el objetivo de que el mayor número de servicios cuenten con parches que cierren esta vulnerabilidad lo antes posible. Pero cibercriminales también hacen lo propio para llevarse uno de los botines más grandes de la historia en el mundo de la ciberseguridad. Es de la mayor urgencia e importancia, no perder tiempo e implementar las medidas de mitigación que han sido recomendadas. Si encuentra anomalías, le sugerimos suponer que se trata de un incidente de ciberseguridad activo y que su organización ha sido comprometida.

En el mundo de la ciberseguridad, pensar **"eso no nos va a pasar" es de los errores más grandes** que se pueden cometer. La buena noticia es que,si fomentamos una conciencia de ciberseguridad y tomamos una postura proactiva para proteger e impulsar el desarrollo y crecimiento de nuestras organizaciones a través de una ciberseguridad sólida y robusta en nuestros cimientos, estaremos un paso adelante que ciberatacantes.

En caso de requerir ayuda con la vulnerabilidad comentada en esta nota, Metabase Q, le puede ayudar detectar si está presente en su infraestructura y detener los ataques.

Sobre todo, a consolidar su base de ciberseguridad con su equipo reforzando su ciberresiliencia.

Autora: Ximena Méndez
heraldodemexico.com.mx