xataka.com

Log4Shell es la vulnerabilidad crítica 'de proporciones catastróficas' que amenaza con destrozar internet

Javier Pastor

3-4 minutos

Estamos ya tan acostumbrados a hablar de robos de datos, fallos de seguridad y vulnerabilidades que hacerlo otra vez parece trivial, pero no lo es. No al menos en el caso de **Log4Shell, una vulnerabilidad zero-day que algunos han calificado como la peor de la historia**.

El problema reside en **Log4j, una librería Java que se usa masivamente en sistemas empresariales y aplicaciones web**. El problema ha afectado ya a servidores de Minecraft que se hackearon con un sencillo mensaje en el chat de la partida, pero la amenaza es enorme para todo tipo de plataformas. Afortunadamente existe parche, así que los administradores de sistemas deberían corregir el problema cuanto antes.

Un problemón contra el que los usuarios finales pueden hacer bien poco (pero sí los

administradores de sistemas)

Log4j es un entorno de trabajo para registro de actividad en Apache y que permite monitorizar la actividad en una aplicación. El CEO de Cloudflare, Matthew Prince, avisó hace unos días de que **el problema era tan gordo** que su empresa trataría de desplegar ciertos mecanismos para mitigarlo incluso para clientes de su servicio gratuito.

Todo lo que tenía que hacer un atacante para explotar el problema es **enviar un pedazo de código malicioso**: ese código acabará siendo registrado por Log4j si está en su versión 2.0 o superior, y al hacerlo dará acceso al atacante al sistema, que podrá ejecutar código de forma remotamente.

Free Wortley, CEO de la plataforma de seguridad LunaSec, explicaba que **este es "un fallo de diseño de proporciones catastróficas" en la librería**, y el problema se explotó por ejemplo en los servidores de Minecraft.

> In the case of Minecraft, attackers were able to get remote code execution on Minecraft Servers by simply pasting a a short message into the chat box.
>
> — Marcus Hutchins (@MalwareTechBlog) December 10,

2021

Varias agencias nacionales de ciberseguridad publicaron alertas sobre el tema, y los expertos avisaban de lo fácil que era exponer especialmente a grandes empresas que usan esa librería de forma habitual. La propia Apache Software Foundation calificó la vulnerabilidad —corregida en Log4j 2.15.0— **con un índice de peligrosidad de 10 sobre 10**.

Lo contaban nuestros compañeros de Genbeta ayer al hablar de cómo **la vulnerabilidad era peculiar por muchas cosas** pero también por una muy llamativa: esa librería, que como decíamos es crítica para muchas plataformas, estaba siendo mantenida por solo tres desarrolladores... en su tiempo libre.

Esos tres desarrolladores lograron atajar el problema y ya han publicado los parches que **permiten a cualquiera administrador de sistema actualizar ese componente de sus sistemas** para evitar que el problema pueda afectar a sus servicios.

Los usuarios finales poco pueden hacer salvo que tengan servidores en los que tengan instalados servicios y aplicaciones que puedan usar ese componente. En ese caso, como los administradores de grandes plataformas y servicios, **la clave está en actualizar los sistemas para que ese componente se corrija** con el parche publicado por esos tres desarrolladores.

Vía | Wired

Más información | CCN-CERT