30.12.2021
DIVISIÓN DE REDES Y SEGURIDAD INFORMÁTICA
CSIRT DE GOBIERNO

Resumen vulnerabilidades Apache Log4j 2

¿Qué es Log4j 2?

- Log4j 2 es una biblioteca de elementos usada por los desarrolladores de software para mantener un registro de actividades o *logging* en diversas aplicaciones. Es muy popular, por lo que se le puede encontrar en todo tipo de software de un gran número de proveedores.

- Algunos ejemplos de programas que usan Log4j2 son algunos tan populares como iCloud, Minecraft y la plataforma de juegos online Steam, e incluso cosas en las que probablemente no pensaríamos, como cargadores de autos eléctricos.

¿Por qué está en las noticias?

- El 9 de diciembre se dio a conocer una **vulnerabilidad** de alta gravedad en **Apache Log4j 2**, una biblioteca de Java ampliamente utilizada alrededor del mundo.

- Las versiones afectadas eran aquellas de la **2.0 a la 2.14.1**. Identificada como **CVE-2021-44228** (y apodada **Log4Shell**), esta vulnerabilidad puede permitir a un atacante ejecutar código de manera remota.

- El 10 de diciembre el CSIRT de Gobierno compartió con la comunidad la existencia de esta vulnerabilidad grave en Log4j 2, **CVE-2021-4428 ("Log4Shell")**[1].

- Para esta vulnerabilidad grave ya existen hoy parches (actualizaciones que corrigen las vulnerabilidades), siendo el más reciente la versión **2.17.1**[2] de Log4j, que además resuelve otras vulnerabilidades menos importantes descubiertas en los últimos días.

¿Qué debemos hacer?

- Los responsables de ciberseguridad de toda organización deben identificar los programas que usan Log4j y actualizarlos cuanto antes, según las instrucciones del proveedor que corresponda. Por eso, el CSIRT también **publicó una lista de enlaces** a los sitios donde los principales proveedores de software informan de cuáles de sus productos usan Log4j[3].

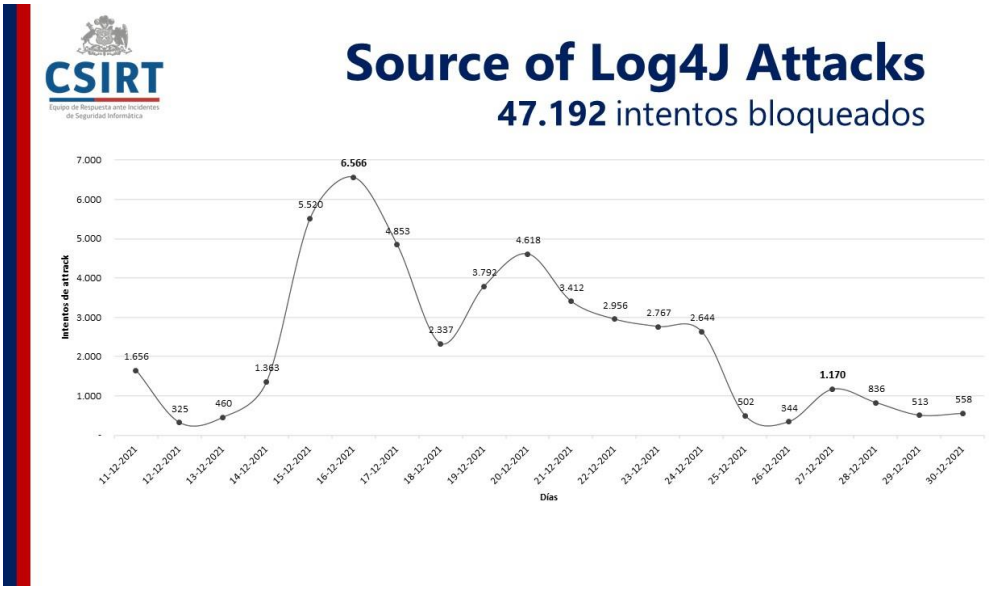
[1] https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00531-01/
[2] https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00539-01/
[3] https://www.csirt.gob.cl/noticias/alerta-apache-log4j-2/

- **Los usuarios no deben asustarse, no hay nada en particular que deban hacer respecto de Logj4, salvo estar atentos a que los productos afectados sean efectivamente parchados**. En este sentido, solo debe seguir las mismas precauciones recomendadas siempre, como **mantener sus aparatos y programas actualizados**, y hacer estas actualizaciones desde **los sitios y tiendas oficiales de sus dispositivos**. Asimismo, es un buen momento para recordar que deben **tener contraseñas seguras y activar el doble factor de autenticación** en sus aparatos y cuentas virtuales.

- Pese a lo extendido del uso de Apache Log4j 2, y la enorme cantidad de ataques registrados que explotan sus vulnerabilidades, no se ha conocido de víctimas prominentes hasta el momento, siendo probablemente la de mayor notoriedad el Ministerio de Defensa de Bélgica[4], entidad que reconoció haber sufrido un ataque que explota Logj4 pero sin dar más detalles.

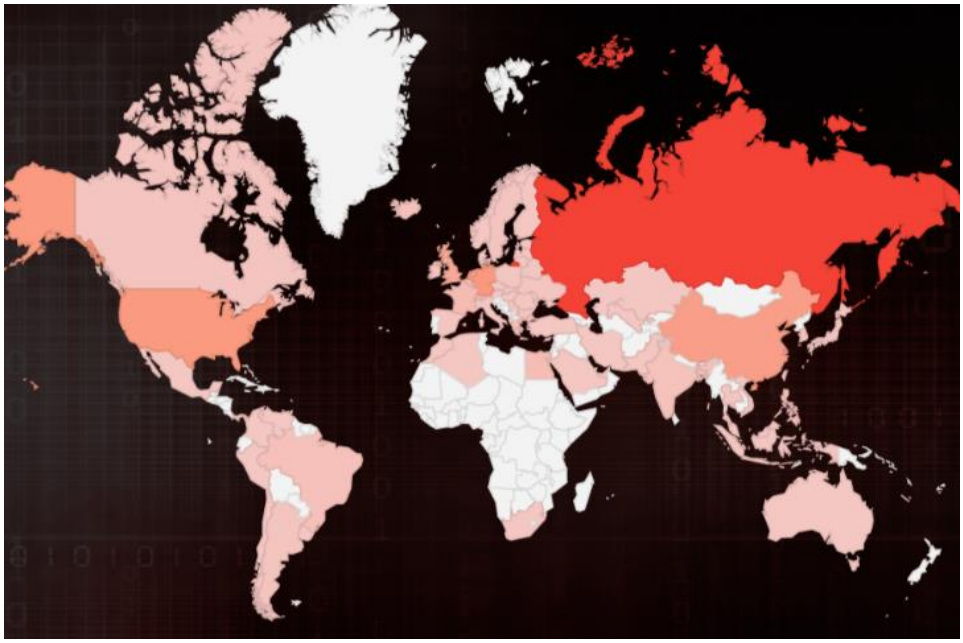
- También se supo de una corredora vietnamita de criptomonedas que sufrió un ransomware (secuestro de archivos digitales) por US$ 5 millones gracias a la explotación de Log4Shell.

- Esta es la evolución de los intentos de ataques relacionados con Log4j a la Red de Conectividad del Estado que han sido detectados al día por el CSIRT de Gobierno durante diciembre. Tras un peak de 6.566 a mediados de mes, se aprecia una tendencia a la baja.



4 https://www.zdnet.com/article/belgian-defense-ministry-confirms-cyberattack-through-log4j-exploitation/.

El principal origen de los ataques detectados a nivel mundial, por el momento, es Rusia (lo que no significa necesariamente que exista una responsabilidad del Estado ruso en estas actividades maliciosas).



CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.12.30 13:25:19 -03'00'