20/12/2021: Descubierta nueva vulnerabilidad crítica asociada a Apache Log4j-2

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, informa con fecha de 20 de diciembre de 2021, de una **nueva vulnerabilidad crítica** que afecta a la librería Apache Log4j 2.

Se trata de una nueva vulnerabilidad con criticidad 9 sobre 10, la **CVE-2021-45046**, y que afecta a la versión 2.15. Esta versión fue propuesta la semana pasada como actualización para solventar la explotación, sin embargo, existe la **versión 2.16 y posterior por lo que recomendamos la actualización a estas últimas.**

Neo4j

Sobre la vulnerabilidad inicial de Log4j, al aplicarse el cambio en la configuración se puede ver afectado Neo4j, para mitigar esta acción la configuración de Neo4j debe ser:

dbms.jvm.additional=-Dlog4j2.formatMsgNoLookups=true

dbms.jvm.additional=-Dlog4j2.disable.jmx=true

Más información: https://community.neo4j.com/t/log4j-cve-mitigation-for-neo4j/48856

Más información sobre la vulnerabilidad en la versión 1.x:

[+] http://slf4j.org/log4shell.html

Más información sobre la vulnerabilidad en la versión 2.x:

https://ws001.sspa.juntadeandalucia.es/confluence/x/4QayBQ

Gracias por su atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud