Nuevos datos 16/12/2021. Vulnerabilidades asociadas a Apache Log4j 2

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las directrices marcadas por el Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, informa de **nue vos datos** respecto a la vulnerabilidad que afecta a la librería Apache Log4j 2.

Asociada a la vulnerabilidad CVE-2021-44228 se ha identificado la vulnerabilidad **CVE-2021-45046**, además de otra (CVE-2021-4104) sobre ***Apache Log4j 1.x*** con ciertos cambios aunque se encuentra relacionada y es explotable.

En **Red Hat** pueden encontrar más información además de cuáles son las clases utilizadas y vulnerables:

[+] https://access.redhat.com/security/cve/CVE-2021-4104

Principalmente, se indica que se tenga en cuenta que este fallo SÓLO afecta a las aplicaciones que están configuradas específicamente para utilizar *JMSAppender*, que no lo es por defecto, o cuando el atacante tiene acceso de escritura a la configuración de Log4j para añadir *JMSAppender* al JMS Broker del atacante.

Cabe destacar que es una vulnerabilidad relacionada con JNDI.

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