Nueva actualización 21/12/2021: Vulnerabilidad crítica en 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 21 de diciembre de 2021, de una **nueva actualización** relacionada con la vulnerabilidad que afecta a la librería **Apache Log4j 2**.

Tras unas semanas en las que se han detectado importantes vulnerabilidades que afectan a Log4j, se ha detectado una **nueva de tipología de denegación de servicio (DoS)**, recogida como **CVE-2021-45105**, por lo que **se recomienda instalar de nuevo parches**, en este caso el **2.17**.

Por ello, se recomienda instalar la última versión disponible para evitar problemas de seguridad. **Este parche** ya está disponible y **permite que las cadenas de búsqueda en la configuración se expandan de forma recursiva**.

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