NEWS

Alert: Active scanning for Apache Log4j 2 vulnerability (CVE-2021-44228)

The NCSC is advising organisations to take steps to mitigate the Apache Log4j 2 vulnerability.

A remote code execution vulnerability (CVE-2021-44228) is affecting multiple versions of the Apache Log4j 2 library. The NCSC is aware that scanning for this vulnerability has been detected in the UK and exploitation detected elsewhere.

Details

Log4j 2 is an open-source Java logging library developed by the Apache Foundation. **It is widely used in many applications and is present in many services as a dependency.** This includes enterprise applications , including custom applications developed within an organisation, as well as numerous cloud services.

The Log4j 2 library is frequently used in enterprise Java software and is included in Apache frameworks including:

- Apache Struts2
- Apache Solr
- Apache Druid
- Apache Flink
- Apache Swift

Other large projects Including **Netty**, **MyBatis** and the **Spring Framework** also make use of the library.

An application which consumes untrusted user input and passes this to a vulnerable version of the Log4j logging library may also be exploited.

Version 1 of the Log4j library is no longer supported and is affected by multiple security vulnerabilities. Developers should migrate to the latest version of Log4j 2.

> More information is available at:
>
> - https://logging.apache.org/log4j/2.x/security.html
> - https://logging.apache.org/log4j/2.x/download.html

Mitigation

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In the case of this vulnerability CVE-2021-44228, **the most important aspect is to install the latest updates as soon as practicable**:

- If you are using the Log4j 2 library as a dependency within an application you have developed, **ensure you update to version 2.15.0 or later**
- If you are using an affected third-party application, **ensure you keep the product updated to the latest version**
- The flaw can also be mitigated in previous releases (2.10 and later) by setting system property "log4j2.formatMsgNoLookups" to "true" or removing the JndiLookup class from the classpath

Advice to vendors of affected software

It may not always be easy for organisations to identify which applications use Apache Log4j 2 software. If you are a vendor of any affected software, the NCSC advises **early communication with your customers** to enable them to apply mitigations or install updates where they are available.

PUBLISHED

10 December 2021

NEWS TYPE

Alert

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals

Was this article helpful?

Yes No