Problem Statement: [1]

log4j is a popular logging library for Java applications. It is used for the high-performance aggregation of log data of an application. The blog of an IT security service provider [LUN2021] reports the vulnerability CVE-2021-44228 [MIT2021] in log4j in versions 2.0 to 2.14.1, which might allow attackers to execute their program code on the target system and thus compromise the server. This might happen when log4j is used to log an attacker-controlled string such as the HTTP User-Agent.

Due to the wide distribution of the library, it is difficult to predict which products are affected.

Measure:

The creator of log4j recommends deleting the class `JndiLookup` from the classpath as a measure that also works in log4j versions 2.0-beta9 and later [APA2021b].

The `JndiLookup` class is not used in Doxis4 and can be removed. Currently there are a number of tools published by the BSI that support this. SER recommends an automated version of the following procedure for mitigation (fixing the vulnerability):

1. Stopping the application
2. Searching for all affected containers (also within WAR containers etc.)
3. Backing up the affected containers
4. Removing the `JndiLookup` class [2]
5. Restarting the application

The BSI and NationalCyberSecurity Centrum NCSC references the following tools to assist in the implementation of the above measures:

- https://github.com/NCSC-NL/log4shell
- https://github.com/NCSC-NL/log4shell/blob/main/scanning/README.md
- https://github.com/logpresso/CVE-2021-44228-Scanner

SER recommends the use of the following tool

- https://github.com/logpresso/CVE-2021-44228-Scanner

taking into account the following instructions:

a) The tool should only be run by administrators who have the appropriate technical background.

b) The tool is only to be applied to the standard Doxis4 installation directories.

c) This measure must first be carried out on the development systems and test systems.

d) Subsequently, final regression tests are to be carried out.

[1] *Note: This document is a technical guide whose content has also been compiled from outside sources. Source BSI:* https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=8

[2] *Deleting the JndiLookup class is considered the better way to go, according to NIST's latest findings. Source NIST CVE-2021-45046:* https://nvd.nist.gov/vuln/detail/CVE-2021-45046

e) Only after successful tests can an application in productive systems take place.

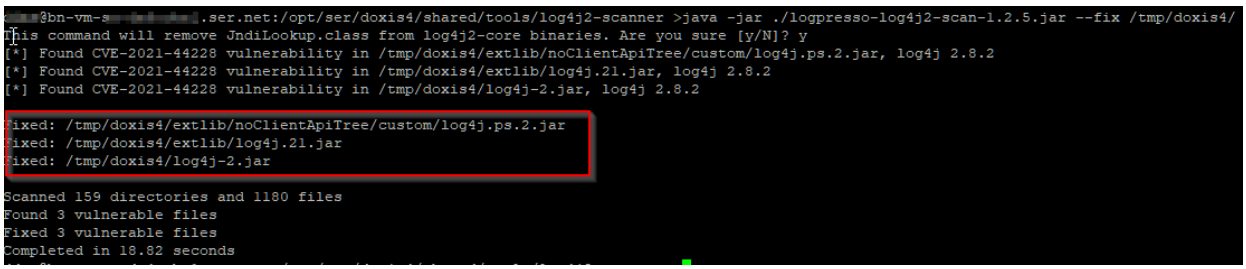
f) Any internal regulations on IT security must be observed in each case. In particular, the responsible internal departments, such as the IT security officer, must be involved as needed.

The tool automatically performs the above steps 2-4 using a specified target path. The overall procedure includes these steps:

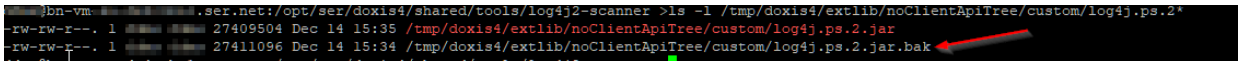
i. Stopp the Doxis4 applications

ii. Run the following command specifying your Doxis4 installation path:
`java -jar logpresso-log4j2-scan.jar --fix --trace target_path_doxis4_installation`

iii. In addition to the corrected versions, there is a `*.bak` file in the same directory, i.e. a backup file for the respective container in the original format. In the output of the command, the corrected versions are listed under the section "fixed".



Example of a `bak file`:



Note: Since the `bak` files can also be loaded by the classloader, they must be removed from the respective directories and saved (in a directory outside of Java classloading). The original path of the `bak` files must be saved as well.

iv. Launch the Doxis4 applications.

We recommend the implementation of the above measures following successful internal tests at SER. We point out that these tests were carried out in a standardized environment. It is not possible to individually map all customer systems.

Fallback scenario:

If problems occur during the above procedure, the original status can be restored by stopping the Doxis4 application and then restoring the affected *. `bak` container. Afterwards, the Doxis4 application must be restarted.