CVE-2021-44228 - Delft-FEWS and Log4J vulnerability

Updated: 6th of January 2022

Statement

Friday, 10 December 2021, our OWASP-scan alerted us to a vulnerability in Log4J, a commonly used open-source library for java applications. https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Analysis Delft-FEWS components and Log4Shell vulnerability CVE-2021-44228.

Worldwide, many java-based applications suffer from the Log4Shell vulnerability CVE-2021-44228. This is caused by a vulnerability in a log4j2 library. The log4j-core-2.11.1.jar is also shipped with the Delft-FEWS software in the 2018.02 - 2021.02 releases. Our users are right in demanding clarity of Deltares whether Delft-FEWS is impacted. Here is our summary of our analysis on the Delft-FEWS software.

- The **Open Archive**, in particular the ElasticSearch and Thredds components with java 8 are vulnerable.
- **Delft-FEWS 2018.02 and later** are NOT vulnerable since the vulnerable method (JNDI lookup) is not executed/executable/runnable from Delft-FEWS.
- Some of the **model adapters** maintained by Deltares are using Log4j2 but they also do not use the vulnerable class (JNDI lookup) nor are they 'open to the outside world' and therefore they are NOT vulnerable either.
- **Tomcat** can only be vulnerable when the applications deployed are vulnerable. The Admin Interface, Webservices, Database Proxy are NOT vulnerable.
- **Older Delft-FEWS versions (2017.02 and before)** are NOT vulnerable for CVE-2021-44228 since log4j version 1.x is used. The log4j 1 version does not have the vulnerable JNDI lookup class but can be vulnerable because of CVE-2021-4104 when someone maliciously configures the JMS appender.
- Deltares supports at maximum 5 versions. If still on 2017.02 or before it is strongly recommended to upgrade to a supported version.
- **JdbcAppenders** as in CVE-2021-44832 are also not executed/executable/runnable from Delft-FEWS.

While Delft-FEWS as such is not directly vulnerable, we do expect virus / security scanners to flag the log4j2 components. We therefore offer updated versions where log4j2 2.11.1 has been replaced with log4j 2.17.

The following fixes and updates are available for Delft-FEWS Stable versions 2019.02 - 2020.01 - 2020.02 - 2021.01 (and release candidate 2021.02) :

- Fixed versions of Elastic Search and Thredds in **Open Archive** distributions.
- Updated distributions (for: **Master Controller, Operator Client/Forecasting Shell Server, Admin Interface, Delft-FEWS Webservices, Database proxy**) with log4j 2.17 .
- Updated distributions for **model adapters** maintained by Delft-FEWS using log4j 2.*: **HEC-HMS, Kanali, Ribasim, SMAP, SWAN, SWMM** and **W ANDA.** The **Delft3D model adapter** is part of the Delft-FEWS code so this one is automatically part of the updated distributions.

Remark: an updated distribution for Delft-FEWS 2018.02 will be made available a.s.a.p.

For more information how to obtain new distributions, please contact fews.support@deltares.nl and visit the installation instruction page (wiki login required).

Delft-FEWS Product Management