Announcement/Log4Shell

Contents

Event

Log4j vulnerability

- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- BSI warning from 12/12/2021 (CVE-2021-44228)

Current vulnerability assessment in BlueSpice (overview)

- BlueSpice free, pro, farm:
  - Current on-premise installations are **not affected**.
  - In older on-premise installations, the **version of Elasticsearch could be affected**.
  - The Docker version is **not affected**.
- BlueSpice Cloud is **not affected**.

This is true for instances that we have installed. **Customers have to check their part of the installation** (i.e., OS, additional packages, etc.)

Inspected components in BlueSpice

Current version

- **ElasticSearch** => ElasticSearch reports that they are not affected: https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
  No code-red alert, but we keep an eye on it. => **not vulnerable**
- **Java-Server**
  - Tomcat => explicit configuration of log4j is necessary. By default, log4j is not activated. We do not change this. => **not vulnerable**
  - Jetty => explicit configuration of jetty is necessary. By default, log4j is not activated. We do not change this. => **not vulnerable**
- **Java Webservices**
  - xhtmlrenderer => a log4j plugin exists, but is not used by our service => **not vulnerable**
  - VisualDiff => uses daisydiff + others. Does not use log4j => **not vulnerable**
  - LaTeX2png => uses the jlatexmath library. Does not use log4j => **not vulnerable**
- **Draw.io** reports that the appication is not affected: https://twitter.com/drawio/status/1470061320066277382 => **not vulnerable**

Older versions of BlueSpice 3

- **Elasticsearch**
  (see https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476)
  - **Versions 6.8.9+**: ElasticSearch is not vulnerable in versions 6.8.9+ which was released on 13th May 2020.
  - **Version 6.4.0 - 6.8.8**: Vulnerable. A configuration change and server restart has to be applied.
  - **Versions 6.3.x and below**: Update of ElasticSearch is required. Please contact our support.

BlueSpice 2

- Solr uses log4j. Currently no mitigation available. Disable Solr search.

Inspected components in the Docker image

The list of Docker files in the activated packages has been inspected. => **not vulnerable**

- https://security-tracker.debian.org/tracker/CVE-2021-44228