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 => **not affected**
  - Older on-premise installations => **version of Elasticsearch could be vulnerable**
  - The Docker version => **not affected**
- BlueSpice Cloud => **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.)

Detailed assessment

Current version

- **Elasticsearch** => **not vulnerable**
  https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
- **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** => **not vulnerable**
  https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
  - **Versions 6.8.9+ (**released on 13th May 2020) => **not vulnerable**
  - **Version 6.4.0 - 6.8.8**: Update of Elasticsearch is recommended.
    => **not vulnerable (updating the version during the next BlueSpice update is recommended)**
    => **vulnerable outside of BlueSpice**

- **Versions 6.3.x and below**: Update of Elasticsearch is recommended.
  => **not vulnerable (updating the version during the next BlueSpice update is recommended)**
  => **vulnerable outside of BlueSpice**

Independently of the Elasticsearch version in use, BlueSpice is not vulnerable due to the setup of Elasticsearch:

- **No direct access:** BlueSpice uses Elasticsearch as an internal service. We set up Elasticsearch in such a way that there cannot be any direct access. The only way to access Elasticsearch if you are not working directly on the server is through BlueSpice, which means there is a very controlled set of access vectors. These are search queries and content which is to be indexed.
- **No logging of data:** We use log level WARN on Elasticsearch, which means no data can find its way to the logs. So there is no way an attacker can add custom information to the logs.

No pass-through of user data: All communication between BlueSpice and Elasticsearch is done user-agnostic. There is no way Elasticsearch can see which user triggers the communication. The user-agent is restricted to the BlueSpice system user.

This is true even if you are running on an older, vulnerable version of Elasticsearch. So we see no urgent action required. Nonetheless, it is recommended to update your Elasticsearch to a non-vulnerable version with the next update of BlueSpice.

If you have changed the Elasticsearch setup to a different log level or loosened the restrictions on Elasticsearch access, you have to check the setup.

BlueSpice 2

- Solr uses log4j => **vulnerable**
  More information on Mitigation is here:
  https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228

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

BlueSpice Cloud

- Swarmpit => **not affected**
- Drone => **not affected**

Related links

- https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html
- https://access.redhat.com/security/vulnerabilities/RHSB-2021-009
- https://www.suse.com/c/suse-statement-on-log4j-log4shell-cve-2021-44228-vulnerability/