Meldung/Log4Shell

Inhaltsverzeichnis

Anlass

Aktuelle log4j Sicherheitslücke.

- BSI Meldung vom 12.12.2021 (CVE-2021-44228)

Berwertung der Schwachstellen in BlueSpice

- BlueSpice free, pro, farm
  - Aktuelle on-Premise Installationen => **nicht betroffen**
  - Ältere on-Premise Installationen => **Elasticsearch könnte verwundbar sein**
  - Docker-Version => **nicht betroffen**
- BlueSpice Cloud => **nicht betroffen**

Dies gilt für die von uns installierten Instanzen. **Kunden müssen ihren Teil der Installation überprüfen** (d.h. Betriebssystem, zusätzliche Pakete, etc.)

Detaillierte Bewertung

Aktuelle Version

- **Elasticsearch** => **nicht verwundbar**
  https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
- **Java-Server**
  - Tomcat => explizite Konfiguration von log4j erforderlich. Im Standard ist log4j nicht aktiviert. Wir ändern das nicht => **nicht verwundbar**
  - Jetty => explizite Konfiguration von jetty erforderlich. Im Standard ist log4j nicht aktiviert. Wir ändern das nicht => **nicht verwundbar**
- **Java Webservices**
  - xhtmlrenderer => es gibt ein log4j Plugin, aber es wird in unserem Service nicht benutzt => **nicht verwundbar**
  - VisualDiff => benutzt daisydiff + andere. Benutzt kein log4j => **nicht verwundbar**
  - LaTeX2png => benutzt jlatexmath Bibliothek. Benutzt kein log4j => **nicht verwundbar**
- **Draw.io** meldet, dass die Anwendung nicht betroffen ist:
  https://twitter.com/drawio/status/1470061320066277382 => **nicht verwundbar**

Ältere Versionen von BlueSpice 3

- **Elasticsearch** => **nicht verwundbar**
  https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476
  - **Versionen 6.8.9+** (Release:13. Mai 2020) => **nicht verwundbar**
  - **Version 6.4.0 - 6.8.8**: Eine Konfigurationsänderung und ein Serverneustart sind empfohlen.
    => **nicht verwundbar (Aktualisierung beim nächsten Update von BlueSpice wird empfohlen)**
    => **nur außerhalb von Bluespice verwundbar**

- **Versionen ≤ 6.3.x**: Ein Update von Elasticsearch ist empfohlen. Bitte kontaktieren Sie unseren Support.
  => **nicht verwundbar (Aktualisierung beim nächsten Update von BlueSpice wird empfohlen)**
  => **nur außerhalb von Bluespice verwundbar**

Unabhängig von der verwendeten ElasticSearch-Version ist BlueSpice aufgrund der Einrichtung von ElasticSearch nicht verwundbar:

- **Kein direkter Zugriff:** BlueSpice verwendet ElasticSearch als internen Service. Die einzige Möglichkeit auf ElasticSearch zuzugreifen, wenn Sie nicht direkt auf dem Server arbeiten, ist über BlueSpice. Das bedeutet, dass es einen sehr kontrollierten Satz von Zugriffsvektoren gibt. Dies sind Suchanfragen und Inhalte, die indiziert werden sollen.
- **Keine Protokollierung von Daten:** Wir verwenden bei ElasticSearch das Log-Level WARN, d. h. keine Daten können den Weg in die Logs finden. Ein Angreifer kann also keine benutzerdefinierten Informationen zu den Protokollen hinzufügen.
- **Keine Weitergabe von Benutzerdaten:** Die gesamte Kommunikation zwischen BlueSpice und ElasticSearch erfolgt benutzerunabhängig. ElasticSearch kann nicht erkennen, welcher Benutzer die Kommunikation auslöst. Der User-Agent ist auf den BlueSpice-Systembenutzer beschränkt.

Dies gilt selbst dann, wenn Sie eine ältere, anfällige Version von ElasticSearch verwenden. Wir sehen daher keinen dringenden Handlungsbedarf. Wir empfehlen, ElasticSearch mit dem nächsten Update von BlueSpice auf eine nicht angreifbare Version zu aktualisieren.

Wenn Sie das ElasticSearch-Setup auf ein anderes Log-Level geändert oder die Einschränkungen für den ElasticSearch-Zugriff gelockert haben, müssen Sie das Setup überprüfen.

BlueSpice 2

- Solr benutzt log4j => **verwundbar**

  Informationen zur Schadensabwendung finden Sie hier:
  https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228

Geprüfte Komponenten im Docker-Image

Die Liste der im Docker-File aktivierten Packages wurde geprüft. => **nicht anfällig**

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

BlueSpice Cloud

- Swarmpit => **nicht betroffen**
- Drone => **nicht betroffen**

Weiterführende 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/