HIGH SEVERITY

Arbitrary Code Execution

- Vulnerable module: ch.qos.logback:logback-classic
- Introduced through: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE

Detailed paths and remediation

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter@1.5.2.RELEASE › org.springframework.boot:spring-boot-starter-logging@1.5.2.RELEASE ›ch.qos.logback:logback-classic@1.1.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@2.0.0.RELEASE.

Unreachable paths

Following modules are not fixable via Snyk as we are unable to reach the relevant files to update them.

- Module: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE
  Location: https://maven-central.storage-download.googleapis.com/repos/central/data/org/springframework/boot/spring-boot-dependencies/1.5.2.RELEASE/spring-boot-dependencies-1.5.2.RELEASE.pom

Overview

Affected versions of `ch.qos.logback:logback-classic` are vulnerable Arbitrary Code Execution via the
the `SocketServer` and `ServerSocketReceiver` components.

A configuration can be turned on to allow remote logging through interfaces that accept untrusted serialized data. Authenticated attackers on the adjacent network can exploit this vulnerability to run arbitrary code through the deserialization of custom gadget chains.

More about this issue

HIGH SEVERITY

Denial of Service (DoS)

- Vulnerable module: org.apache.tomcat.embed:tomcat-embed-core
- Introduced through: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE

Detailed paths and remediation

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-websocket@8.5.11 ›org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

Unreachable paths

Following modules are not fixable via Snyk as we are unable to reach the relevant files to update them.

- Module: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE
  Location: https://maven-central.storage-download.googleapis.com/repos/central/data/org/springframework/boot/spring-boot-dependencies/1.5.2.RELEASE/spring-boot-dependencies-1.5.2.RELEASE.pom

Overview

`org.apache.tomcat.embed:tomcat-embed-core` In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the handling of an HTTP/2 GOAWAY frame for a connection did not close streams associated with that connection that were currently waiting for a `WINDOW_UPDATE` before allowing the application to write more data. These waiting streams each consumed a thread. A malicious client could therefore construct a series of HTTP/2 requests that would consume all available processing threads.

More about this issue
HIGH SEVERITY

Information Disclosure

- Vulnerable module: org.apache.tomcat.embed:tomcat-embed-core
- Introduced through: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE

Detailed paths and remediation

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-websocket@8.5.11 ›org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

Unreachable paths

Following modules are not fixable via Snyk as we are unable to reach the relevant files to update them.

- Module: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE
  Location: https://maven-central.storage-download.googleapis.com/repos/central/data/org/springframework/boot/spring-boot-dependencies/1.5.2.RELEASE/spring-boot-dependencies-1.5.2.RELEASE.pom

Overview

`org.apache.tomcat.embed:tomcat-embed-core` is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies.

Affected versions of this package are vulnerable to Information Disclosure. A bug in the handling of the pipelined requests, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.

More about this issue

HIGH SEVERITY

Information Disclosure

- Vulnerable module: org.apache.tomcat.embed:tomcat-embed-core
- Introduced through: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE

Detailed paths and remediation

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-websocket@8.5.11 ›org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

Unreachable paths

Following modules are not fixable via Snyk as we are unable to reach the relevant files to update them.

- Module: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE
  Location: https://maven-central.storage-download.googleapis.com/repos/central/data/org/springframework/boot/spring-boot-dependencies/1.5.2.RELEASE/spring-boot-dependencies-1.5.2.RELEASE.pom

Overview

`org.apache.tomcat.embed:tomcat-embed-core` is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies.

Affected versions of this package are vulnerable to Information Disclosure. While investigating bug 60718, it was noticed that some calls to application listeners, It did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore

possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.

More about this issue

HIGH SEVERITY

Information Disclosure

- Vulnerable module: org.apache.tomcat.embed:tomcat-embed-core
- Introduced through: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE

Detailed paths and remediation

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-websocket@8.5.11 ›org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

- Introduced through: com.example.r42:suchapp@0.0.1-SNAPSHOT › org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE ›org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE › org.apache.tomcat.embed:tomcat-embed-core@8.5.11
  Remediation: Upgrade to org.springframework.boot:spring-boot-starter-web@1.5.3.RELEASE.

Unreachable paths

Following modules are not fixable via Snyk as we are unable to reach the relevant files to update them.

- Module: org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE
  Location: https://maven-central.storage-download.googleapis.com/repos/central/data/org/springframework/boot/spring-boot-dependencies/1.5.2.RELEASE/spring-boot-dependencies-1.5.2.RELEASE.pom

Overview

`org.apache.tomcat.embed:tomcat-embed-core` In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the refactoring of the HTTP connectors introduced a regression in the send file processing. If the send file processing completed quickly, it was

possible for the Processor to be added to the processor cache twice. This could result in the same Processor being used for multiple requests which in turn could lead to unexpected errors and/or response mix-up.

- Dependencies with issues

com.example.r42:suchapp
org.springframework.boot:spring-boot-starter-web@1.5.2.RELEASE
org.springframework.boot:spring-boot-starter@1.5.2.RELEASE
org.springframework.boot:spring-boot-starter-logging@1.5.2.RELEASE


ch.qos.logback:logback-classic@1.1.11
org.springframework.boot:spring-boot-starter-tomcat@1.5.2.RELEASE


org.apache.tomcat.embed:tomcat-embed-core@8.5.11
org.apache.tomcat.embed:tomcat-embed-websocket@8.5.11


org.apache.tomcat.embed:tomcat-embed-core@8.5.11