resteasy/Resteasy:resteasy-jsapi-testing/pom.xml

READ-ONLY

Overview History Settings

Snapshot taken by snyk.io 12 hours ago.

Vulnerabilities	5 via 30 paths
Dependencies	46
Source	GitHub
Taken by	Web
Repository	Resteasy
Branch	master
Manifest	resteasy-jsapi-testing/pom.xml

HIGH SEVERITY

Information Disclosure

Vulnerable module: io.netty:netty

Introduced through: org.seleniumhq.selenium:selenium-java@2.51.0

Detailed paths

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-safari-driver@2.51.0 › org.webbitserver:webbit@0.4.14 › io.netty:netty@3.5.2.Final

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.webbitserver:webbit@0.4.14 › io.netty:netty@3.5.2.Final

Overview

io.netty:netty is a NIO client server framework which enables quick and easy development of network applications such as protocol servers and clients.

Affected versions of this package are vulnerable to Information Disclosure. It does not validate cookie name and value characters, allowing attackers to potentially bypass the `httpOnly` flag on sensitive cookies.

HIGH SEVERITY

Timing Attack

Vulnerable module: org.eclipse.jetty:jetty-util

Introduced through: org.seleniumhq.selenium:selenium-java@2.51.0

Detailed paths

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 › net.sourceforge.htmlunit:htmlunit@2.18 › org.eclipse.jetty.websocket:websocket-client@9.2.12.v20150709 › org.eclipse.jetty.websocket:websocket-common@9.2.12.v20150709 › org.eclipse.jetty:jetty-io@9.2.12.v20150709 › org.eclipse.jetty:jetty-util@9.2.12.v20150709

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 › net.sourceforge.htmlunit:htmlunit@2.18 › org.eclipse.jetty.websocket:websocket-client@9.2.12.v20150709 › org.eclipse.jetty.websocket:websocket-common@9.2.12.v20150709 › org.eclipse.jetty:jetty-util@9.2.12.v20150709

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 › net.sourceforge.htmlunit:htmlunit@2.18 › org.eclipse.jetty.websocket:websocket-client@9.2.12.v20150709 › org.eclipse.jetty:jetty-io@9.2.12.v20150709 › org.eclipse.jetty:jetty-util@9.2.12.v20150709

…and 1 more

Overview

org.eclipse.jetty:jetty-util is a lightweight highly scalable java based web server and servlet engine.

Affected versions of this package are vulnerable to Timing Attacks. A flaw in the `util/security/Password.java` class makes it easier for remote attackers to obtain access by observing elapsed times before rejection of incorrect passwords.

MEDIUM SEVERITY

Deserialization of Untrusted Data

Vulnerable module: com.google.guava:guava

Introduced through: org.seleniumhq.selenium:selenium-java@2.51.0 and org.seleniumhq.selenium:selenium-chrome-driver@2.51.0

Detailed paths

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 › org.seleniumhq.selenium:selenium-support@2.51.0 › org.seleniumhq.selenium:selenium-remote-driver@2.51.0 › org.seleniumhq.selenium:selenium-api@2.51.0 › com.google.guava:guava@19.0

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-firefox-driver@2.51.0 › org.seleniumhq.selenium:selenium-remote-driver@2.51.0 › org.seleniumhq.selenium:selenium-api@2.51.0 › com.google.guava:guava@19.0

Remediation: Upgrade to org.seleniumhq.selenium:selenium-java@3.0.0

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-edge-driver@2.51.0 › org.seleniumhq.selenium:selenium-remote-driver@2.51.0 › org.seleniumhq.selenium:selenium-api@2.51.0 › com.google.guava:guava@19.0

Remediation: Upgrade to org.seleniumhq.selenium:selenium-java@3.0.0

…and 15 more

Overview

com.google.guava:guava is a set of core libraries that includes new collection types (such as multimap and multiset,immutable collections, a graph library, functional types, an in-memory cache and more.

Affected versions of this package are vulnerable to Deserialization of Untrusted Data.

During deserialization, two Guava classes accept a caller-specified size parameter and eagerly allocate an array of that size:

`AtomicDoubleArray` (when serialized with Java serialization)
`CompoundOrdering` (when serialized with GWT serialization)
An attacker may be able to send a specially crafted request which with then cause the server to allocate all it's memory, without validation whether the data size is reasonable.

MEDIUM SEVERITY

Denial of Service (DoS)

Vulnerable module: io.netty:netty

Introduced through: org.seleniumhq.selenium:selenium-java@2.51.0

Detailed paths

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.webbitserver:webbit@0.4.14 › io.netty:netty@3.5.2.Final

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-safari-driver@2.51.0 › org.webbitserver:webbit@0.4.14 › io.netty:netty@3.5.2.Final

Overview

io.netty:netty is a NIO client server framework which enables quick and easy development of network applications such as protocol servers and clients.

Affected versions of this package are vulnerable to Denial of Service (DoS) The SslHandler in Netty before 3.9.2 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted SSLv2Hello message.

MEDIUM SEVERITY

Cross-site Scripting (XSS)

Vulnerable module: org.eclipse.jetty:jetty-util

Introduced through: org.seleniumhq.selenium:selenium-java@2.51.0

Detailed paths

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 › net.sourceforge.htmlunit:htmlunit@2.18 › org.eclipse.jetty.websocket:websocket-client@9.2.12.v20150709 › org.eclipse.jetty.websocket:websocket-common@9.2.12.v20150709 › org.eclipse.jetty:jetty-io@9.2.12.v20150709 › org.eclipse.jetty:jetty-util@9.2.12.v20150709

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 ›

net.sourceforge.htmlunit:htmlunit@2.18 › org.eclipse.jetty.websocket:websocket-client@9.2.12.v20150709 › org.eclipse.jetty.websocket:websocket-common@9.2.12.v20150709 › org.eclipse.jetty:jetty-util@9.2.12.v20150709

Introduced through: org.jboss.resteasy:resteasy-jsapi-testing@4.1.0-SNAPSHOT › org.seleniumhq.selenium:selenium-java@2.51.0 › org.seleniumhq.selenium:selenium-htmlunit-driver@2.51.0 › net.sourceforge.htmlunit:htmlunit@2.18 › org.eclipse.jetty.websocket:websocket-client@9.2.12.v20150709 › org.eclipse.jetty:jetty-io@9.2.12.v20150709 › org.eclipse.jetty:jetty-util@9.2.12.v20150709

…and 1 more

Overview

org.eclipse.jetty:jetty-util is a Web Container & Clients - supports HTTP/2, HTTP/1.1, HTTP/1.0, websocket, servlets, and more.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS) when a remote client uses a specially formatted URL against the `DefaultServlet` or `ResourceHandler` that is configured for showing a listing of directory contents.

© 2019 Snyk Ltd.