

Verifying Hidden Reapers

Spice Labs has discovered thousands of [Hidden Reapers](#)... software artifacts that contain vulnerabilities not flagged by GitHub Dependabot or other vulnerability scanning software.

This is a quick guide to show you how to verify Spice Labs' claims.

Claimed Reaper Artifacts

Software components, also called artifacts, can be identified by a "[Package URL](#)" or pURL.

You should have received a text file that's also a machine readable "JSON" file that contains a set of Hidden Reapers. Each of the artifacts with a Hidden Reaper has an "artifact" field. For example:

```
"artifact": "pkg:maven/ca.uhnresearch.pughlab/java-server@1.0.5"
```

This field can be used to look up information about the artifact in a 3rd party site, MVN Repository. The link to look up the artifact is also included:

```
"mvnrepository": "https://mvnrepository.com/artifact/ca.uhnresearch.pughlab/java-server/1.0.5"
```

By clicking on the link, you can see the dependencies and vulnerability information. There are no listed dependencies for

```
"pkg:maven/ch.qos.logback/logback-classic@1.1.8",
```

```
"pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@8.0.0-RC10", or
```

```
"pkg:maven/ch.qos.logback/logback-core@1.1.8"
```

And the [Common Vulnerabilities and Exposures](#) (CVEs) associated with the Hidden dependencies are not listed.

Confirming the Reapers are Hidden

You can verify that the above packages (e.g., logback-core 1.1.8) are embedded in the code.

First, download the JAR file (the computer code) by clicking on the "jar (7.2MB)" link:

Home » [ca.uhnresearch.pughlab](#) » [java-server](#) » 1.0.5



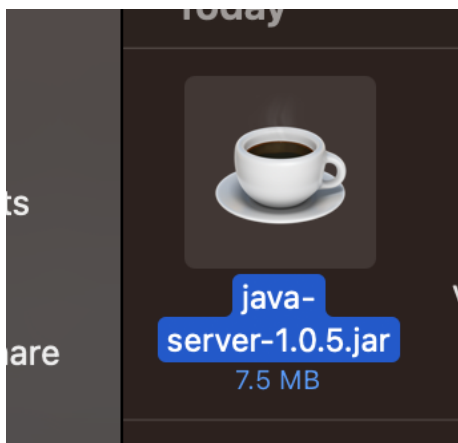
Generic Server Container » 1.0.5

A generic server container for the tracker, cbioPortal, and other Java-base

License	BSD 3-clause
Tags	server
HomePage	https://github.com/pughlab/java-server
Date	Jan 12, 2017
Files	pom (7 KB) jar (7.2 MB) View All

Next, open the file using a Zip file tool because Java JAR files are just Zip files. For the purposes of this document, we are using [Trend Micro's Unzip One](#) on a Mac.

In your Download file, right-click on the “java-server-1.0.5.jar” file:



And select “Open With > Unzip One.app”

You should see the contents of the JAR file:

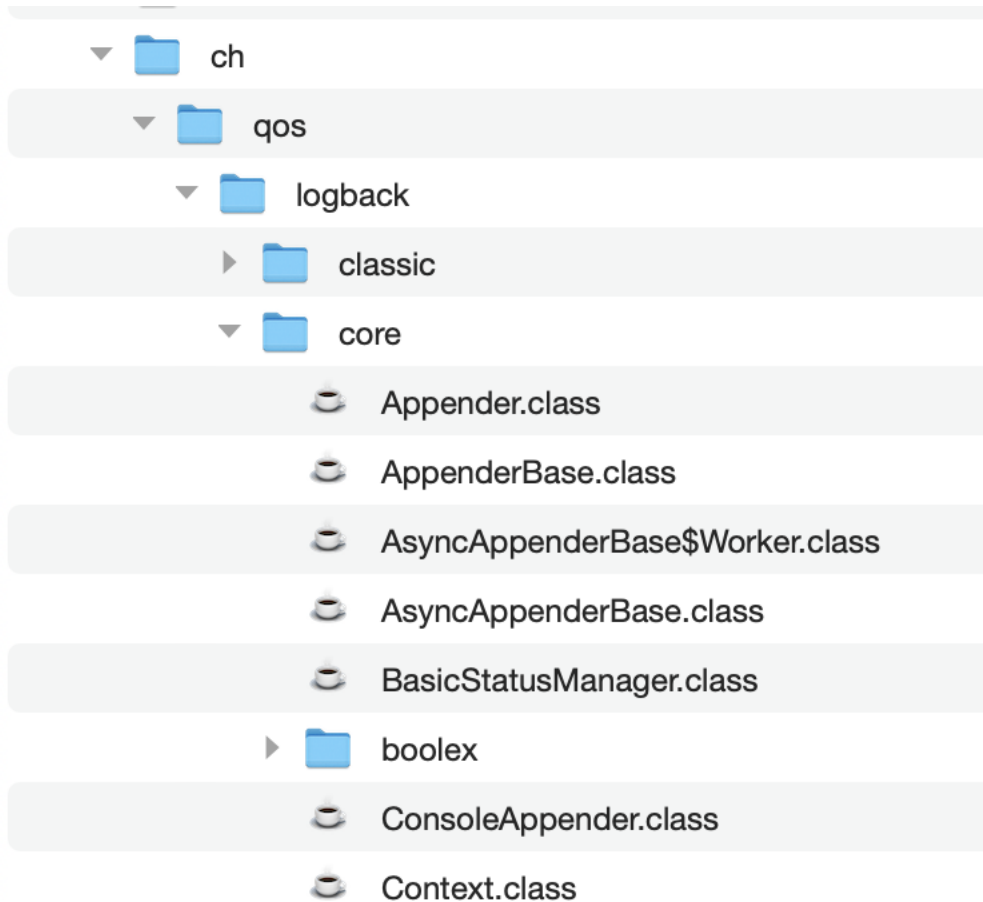
java-server-1.0.5.jar

New Extract Secure Extract Compress Fast Share Settings Toolbox Support

Did you know that \$43 billion was lost to identity theft in the US in 2022? Find out if your email address and phone number have been leaked on the dark web. [Check Now](#)

Name	Size	Date Modified	Kind
java-server-1.0.5.jar	7.00 MB	Sep 12, 2024 at 9:34 AM	Java archive
▶ META-INF	--	Jan 12, 2017 at 11:15 AM	folder
▶ ca	--	Jan 12, 2017 at 11:15 AM	folder
jetty-logging.properties	99 B	Jan 12, 2017 at 11:15 AM	
logback.xml	1.00 KB	Jan 12, 2017 at 11:15 AM	XML text
▶ javax	--	Jan 12, 2017 at 11:15 AM	folder
▶ org	--	Jan 12, 2017 at 11:15 AM	folder
about.html	2.00 KB	Jan 12, 2017 at 11:15 AM	HTML text
jndi.properties	125 B	Jan 12, 2017 at 11:15 AM	
jetty-dir.css	319 B	Jan 12, 2017 at 11:15 AM	CSS
▶ com	--	Jan 12, 2017 at 11:15 AM	folder
testpool.jocl	2.00 KB	Jan 12, 2017 at 11:15 AM	
▶ ch	--	Jan 12, 2017 at 11:15 AM	folder

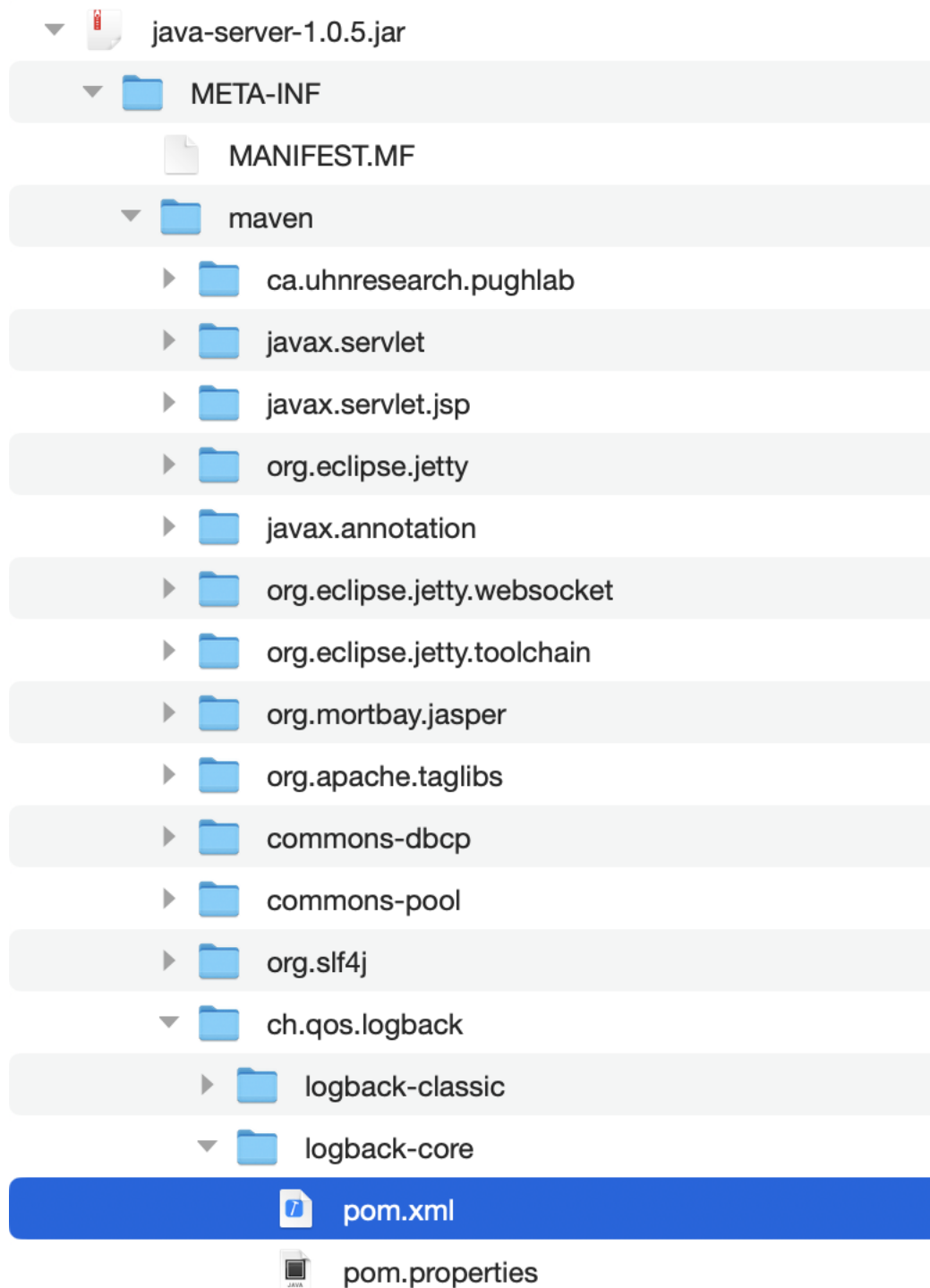
Within the JAR file, you can see directories for “ch”. Click to open the directory:



You can see that the class files exist for the package that's not listed.

Next, let's make sure that it's really [logback core 1.1.8](#), an artifact with a critical vulnerability.

Navigate through META-INF > Maven > ch.qos.logback > logback-core and extract the "pom.xml" file.



Open the `pom.xml` file with `TextEdit.app` and note that the file is based on `logback 1.18`:

```
<parent>
  <groupId>ch.qos.logback</groupId>
  <artifactId>logback-parent</artifactId>
  <version>1.1.8</version>
</parent>
```

Thus, you can confirm the Hidden Reaper exists in the file yet it is not listed as a dependency and its critical vulnerability is not included in any package information.