eclipse / **jetty.project** Public

Code Issues 372 Pull requests 14 Actions Projects 7 **Security 12**

SslConnection does not release pooled ByteBuffers in case of errors

High **waynebeaton** published **GHSA-8mpp-f3f7-xc28** on Jul 7

Package

jetty-server (Maven)

Affected versions	Patched versions
10.0.0 to 10.0.9, 11.0.0 to 11.0.9	10.0.10, 11.0.10

Description

Impact

`SslConnection` does not release `ByteBuffer` s in case of error code paths.
For example, TLS handshakes that require client-auth with clients that send expired certificates will trigger a TLS handshake errors and the `ByteBuffer` s used to process the TLS handshake will be leaked.

Versions Impacted

Jetty Server 10.0.0 to 10.0.9
Jetty Server 11.0.0 to 10.0.9

Workarounds

Configure explicitly a `RetainableByteBufferPool` with `max[Heap|Direct]Memory` to limit the amount of memory that is leaked.
Eventually the pool will be full of "active" entries (the leaked ones) and will provide `ByteBuffer` s that will be GCed normally.

With embedded-jetty

```
int maxBucketSize = 1000;
long maxHeapMemory = 128 * 1024L * 1024L; // 128 MB
long maxDirectMemory = 128 * 1024L * 1024L; // 128 MB
RetainableByteBufferPool rbbp = new ArrayRetainableByteBufferPool(0, -1, -1, maxBucketSize, maxH
server.addBean(rbbp); // make sure the ArrayRetainableByteBufferPool is added before the server
server.start();
```

With jetty-home/jetty-base

Create a `${jetty.base}/etc/retainable-byte-buffer-config.xml`

```
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN" "https://www.eclipse.org/jetty/configure_10

<Configure id="Server" class="org.eclipse.jetty.server.Server">
  <Call name="addBean">
    <Arg>
      <New class="org.eclipse.jetty.io.ArrayRetainableByteBufferPool">
        <Arg type="int"><Property name="jetty.byteBufferPool.minCapacity" default="0"/></Arg>
        <Arg type="int"><Property name="jetty.byteBufferPool.factor" default="-1"/></Arg>
        <Arg type="int"><Property name="jetty.byteBufferPool.maxCapacity" default="-1"/></Arg>
        <Arg type="int"><Property name="jetty.byteBufferPool.maxBucketSize" default="1000"/></Ar
        <Arg type="long"><Property name="jetty.byteBufferPool.maxHeapMemory" default="128000000"
        <Arg type="long"><Property name="jetty.byteBufferPool.maxDirectMemory" default="12800000
      </New>
    </Arg>
  </Call>
</Configure>
```

And then reference it in `${jetty.base}/start.d/retainable-byte-buffer-config.ini`

```
etc/retainable-byte-buffer-config.xml
```

References

#8161

For more information

- Email us at security@webtide.com

Severity

High 7.5 / 10

CVSS base metrics

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2022-2191

Weaknesses

CWE-404 CWE-664