HTTP/2 client can force the server to allocate a humongous byte buffer that may lead to OoM and subsequently the JVM to exit

High **joakime** published **GHSA-889j-63jv-qhr8** 2 days ago

Package	Affected versions	Patched versions
org.eclipse.jetty.http2:jetty-http2-common (Maven)	>=12.0.0, <=12.0.16	12.0.17

Description

Original Report

Bjørn Seime bjorncs@vespa.ai
10:27 AM (10 minutes ago)

Hi.

We've identified a potential denial of service vulnerability affecting Jetty HTTP/2 servers on 12.0.16.

A HTTP/2 client can force the server to allocate a humongous byte buffer that may lead to OoM and subsequently the JVM to exit.

See attached zip file for readme and a full proof of concept.

--
Bjorn C Seime
Vespa.ai, Trondheim - Norway

Impact

Remote peers can cause the JVM to crash or continuously report OOM.

Patches

12.0.17

Severity

High 7.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2025-1948

Weaknesses

CWE-400

Credits

bjorncs Reporter

Workarounds

No workarounds.

References

#12690