[Eclipse Jetty] HTTP/2 clients can force excessive memory allocation on server

Closed Issue created 2 months ago by **Simone Bordet**

The Eclipse Foundation is a Common Vulnerabilities and Exposures (CVE) Numbering Authority. This issue it used to request and track the progress of the assignment of a CVE for a vulnerability in the project code for an Eclipse open source project.

Basic information

Project name: Eclipse Jetty

Project id: rt/jetty

Request type: reservation

Versions affected: [12.0.0, 12.0.16]

Common Weakness Enumeration:

- CWE-400

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

Summary:

In Eclipse Jetty versions 12.0.0 to 12.0.16 included, an HTTP/2 client can specify a very large value for the HTTP/2 settings parameter SETTINGS_MAX_HEADER_LIST_SIZE. The Jetty HTTP/2 server does not perform validation on this setting, and tries to allocate a ByteBuffer of the specified capacity to encode HTTP responses, likely resulting in OutOfMemoryError being thrown, or even the JVM process exiting.

Links:

- https://github.com/jetty/jetty.project/security/advisories/GHSA-889j-63jv-qhr8
- https://github.com/jetty/jetty.project/issues/12690

Tracking

This section will completed by the project team.

☑ Reserve an entry only
☑ We're ready for this issue to be reported to the central authority (i.e., make this public now)
☑ (when applicable) The GitHub Security Advisory is ready to be published now

Note that for those projects that host their repositories on GitHub, the use of GitHub Security Advisories is recommended but is not required.

This section will be completed by the EMO.

CVE: {cve}

□ All required information is provided
□ CVE Assigned
□ Pushed to Mitre
□ Accepted by Mitre

3 of 7 checklist items completed · Edited 2 weeks ago by Joakim Erdfelt

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

No child items are currently assigned. Use child items to break down this issue into smaller parts.

Link issues together to show that they're related or that one is blocking others. Learn more.

Activity

Marta Rybczynska @mrybczyn · 2 months ago Maintainer

Hello, we're going to use CVE-2025-1948 for this one

Marta Rybczynska added cve reserved label 2 months ago

Mikaël Barbero assigned to @jerdfelt 2 weeks ago

Joakim Erdfelt @jerdfelt · 2 weeks ago

We are good with publishing this CVE at this point in time. (along with publishing the associated github advisory)

Joakim Erdfelt marked the checklist item **We're ready for this issue to be reported to the central authority (i.e., make this public now)** as completed 2 weeks ago

Joakim Erdfelt marked the checklist item **(when applicable) The GitHub Security Advisory is ready to be published now** as completed 2 weeks ago

Joakim Erdfelt @jerdfelt · 4 days ago

ping. what's the status on this?

Tiago Lucas @tiagolucas · 1 day ago Developer

The CVE has been published: https://www.cve.org/cverecord?id=CVE-2025-1948
Removing the confidentiality from this issue. Would you like me to publish the Github Advisory @jerdfelt ?

Edited 1 day ago by Tiago Lucas

Joakim Erdfelt @jerdfelt · 1 day ago

Thanks.
I'll publish the github advisory side.
I will update here when things are done.

Please register or sign in to reply

Tiago Lucas made the issue visible to everyone 1 day ago

Joakim Erdfelt @jerdfelt · 1 day ago

The publishing of the github advisory and announcements have been completed.
Feel free to remove confidentiality and close this issue at your convenience.

Tiago Lucas added cve published label and removed cve reserved label 1 day ago

⊖ **Tiago Lucas** closed 1 day ago

Please register or sign in to reply