

undertow-io / undertow Public

<> Code Pull requests 45 Actions Projects Security and quality Insights

[UNDERTOW-2598] CVE-2025-9784 Prevent a MadeYouReset HTTP2 attack by ... #1778

Merged fl4via merged 4 commits into undertow-io:main from fl4via:UNDERTOW-2598 on Oct 10, 2025

Conversation 8 Commits 4 Checks 13 Files changed 6

fl4via commented on Sep 4, 2025 • edited Member

...sending a go away in case too many rst streams were sent to the client.

Jira: <https://issues.redhat.com/browse/UNDERTOW-2598>

Followed-up by #1804
2.3.x PRs: #1802 #1803
2.2.x PR: #1805

👍 1 👁 1

fl4via added bug fix next release labels on Sep 4, 2025

fl4via force-pushed the UNDERTOW-2598 branch from 8289559 to 6343e3e 8 months ago Compare

fl4via added the on hold label on Sep 4, 2025

usr42 commented on Sep 9, 2025

Is CVE-2025-9784 already fixed in version 2.3.19.Final like suggested in <https://issues.redhat.com/browse/UNDERTOW-2598>? Or does this PR needs to be merged first and a version 2.3.20.Final needs to be released to fix the CVE?

marcosgopen commented [on Sep 10, 2025](#)

Is [CVE-2025-9784](#) already fixed in version 2.3.19.Final like suggested in <https://issues.redhat.com/browse/UNDERTOW-2598>? Or does this PR needs to be merged first and a version 2.3.20.Final needs to be released to fix the CVE?

I think this still needs to be fixed (the issue is code in progress).

gdiazsnap commented [on Sep 17, 2025](#)

Hi, is there any plan to release this fix soon?



wolfkor commented [on Sep 23, 2025](#)

We are also urgently waiting for a hotfix to resolve this high severity vulnerability

lsainisnap commented [on Sep 23, 2025](#)

We're also eagerly awaiting a hotfix to fix this serious vulnerability. please merge and provide new fix version

1kvsn commented [on Sep 23, 2025](#)

Hey team, are we going to fix this soon ?


fl4via commented [on Oct 3, 2025](#)

Member

Author


Hello everyone! This fix has not passed all my tests and we have been working on finding the missing pieces. I am working on an updated version of this fix, one that contains those missing pieces.



 fl4via added the **waiting PR update** label on Oct 3, 2025

 fl4via force-pushed the **UNDERTOW-2598** branch from **6343e3e** to **e5730dc** 7 months ago Compare

 fl4via added **waiting CI check** and removed **on hold** **waiting PR update** labels on Oct 9, 2025

 fl4via force-pushed the **UNDERTOW-2598** branch 2 times, most recently from **4ef6a34** to **3760596** 7 months ago Compare

 fl4via added 2 commits 7 months ago

 [UNDERTOW-2598] [CVE-2025-9784](#) Prevent a MadeYouReset HTTP2 attack by ... d00279a

 [UNDERTOW-2598] [CVE-2025-9784](#) Prevent the dispatch of an exchange if ... b595901

 fl4via force-pushed the **UNDERTOW-2598** branch from **3760596** to **e00c48a** 7 months ago Compare

 fl4via added 2 commits 7 months ago


 [UNDERTOW-2598] [CVE-2025-9784](#) Add a delay in the actual direct byte b... fd9bade


 [UNDERTOW-2598] [CVE-2025-9784](#) At AbstractFramedStreamSinkChannel, saf... ✓ 294ea0d

 fl4via force-pushed the **UNDERTOW-2598** branch from **e00c48a** to **294ea0d** 7 months ago Compare

 fl4via mentioned this pull request on Oct 10, 2025

[UNDERTOW-2607][UNDERTOW-2604][UNDERTOW-2235][UNDERTOW-2598] CVE-2025-9784 Backport fixes to 2.3.x #1802

 Merged

 fl4via removed the **waiting CI check** label on Oct 10, 2025



fl4via merged commit 8dbd44c into undertow-io:main on Oct 10, 2025

View details

13 checks passed



fl4via deleted the UNDERTOW-2598 branch 7 months ago

wolfkor commented on Oct 10, 2025

spring-boot is using 2.3.19.Final but that is not official and still has the vulnerability inside



fl4via mentioned this pull request on Oct 10, 2025

[UNDERTOW-2235][UNDERTOW-2598][UNDERTOW-2604] [UNDERTOW-2607] [UNDERTOW-2608] CVE-2025-9784 Backport fixes to 2.2.x #1805

Merged



fl4via mentioned this pull request on Oct 10, 2025

[UNDERTOW-2598] CVE-2025-9784 Replace the delayed cleaning algorithm in DirectByteB... #1804

Merged



fl4via removed the next release label on Oct 10, 2025



fl4via mentioned this pull request on Oct 11, 2025

[UNDERTOW-2598] CVE-2025-9784 Replace the delayed cleaning algorithm in DirectByteB... #1803

Merged

Sign up for free to join this conversation on GitHub. Already have an account? Sign in to comment

Reviewers

No reviews

Assignees

No one assigned

Labels



Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

7 participants

