{ }

Vespa Blog

The AI Search Platform

SUBSCRIBE



Kristian Aune

Head of Customer Success, Vespa.ai

11 Oct 2023

HTTP/2 Rapid Reset (CVE-2023-44487)

2023-10-10, details of the vulnerability now named HTTP/2 Rapid Reset (CVE-2023-44487) were announced. This vulnerability impacts most HTTP/2 servers in the industry, including Vespa by embedding Jetty.

Jetty-11.0.17 which addresses this vulnerability was available 2023-10-10 04:19 UTC. Vespa 8.240.5 was subsequently built and released to Vespa Cloud same day.

If you are using Vespa Cloud, no action is needed, as you have already been upgraded to the safe release.

If you are self-hosting, you are advised to upgrade to Vespa 8.240.5 as soon as possible.

For any questions, meet the Vespa Team at slack.vespa.ai.

Read more:

- cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/
- cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack

Read more

« Vespa is becoming a company
Introducing Lucene Linguistics »

Share

Copyright © 2026 Vespa Blog - Subscribe to updates - Vespa Blog RSS feed - Cookie Preferences

Mediumish Jekyll Theme by WowThemes.net

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy