Is Traefik vulnerable to CVE-2023-44487?

kubernetes-ingress, kubernetes-crd

trinhpham 1 October 11, 2023, 4:57am

I use Traefik 2.x as the Ingress Controller for my production K8s cluster. Therefore, I'd like to know if it's vulnerable to **CVE-2023-44487** or not.

Thanks for your reply 🙂

High memory usage during DoS

blanebramble 2 October 11, 2023, 7:35am

Can we also have a comment on Traefik 1.7 regarding CVE-2023-44487

nicomengin 3 October 11, 2023, 8:34am

Hello @trinhpham , @blanebramble ,

Thanks for reaching out.

We are currently working on a fix for Traefik v2.10, we'll keep you updated about it once the new version is available.

As Traefik v1 is not maintained anymore, we haven't planned to bring the fix to Traefik v1.7.
You can find the list of the supported versions in **the documentation**.

js285 4 October 11, 2023, 8:40am

Hello @nicomengin ,

Thanks for keeping us updated.

Since this vulnerability has had a far reaching impact all around (Cloudflare, Google and AWS were affected) and the fix for Traefik is still to be relased, could you provide some guidance in the meanwhile on how to workdaround/mitigate this vulnerability?

svx 5 October 12, 2023, 12:47pm

Hi @trinhpham @blanebramble and @js285

New versions of Traefik v2.10 and v3-beta are available on **GitHub**.

jokke 6 October 12, 2023, 2:19pm

Hi svx,

Neither of the v2.10.5 nor the v3 beta4 release notes mention fix for the CVE, can you please confirm that the fix was included in v2.10.5 (released yesterday), pointer to the commit addressing this would be super helpful.

Thanks,
jokke

ldez 7 October 12, 2023, 2:38pm

The fix is included in the 2 versions (v2.10.5 and v3.0.0-beta4).

jokke 8 October 12, 2023, 2:41pm

Thanks all for swift response and fix for this vulnerability. Amazing work.

nicomengin 9 October 13, 2023, 8:19am

Hello @jokke,

Thanks for reaching out, we have updated both changelogs to add this information.
Moreover, we have published a **topic** summarizing the actions done to fix the CVEs.

Jancis 10 October 16, 2023, 6:45am

I was unable to pinpoint the actual fix in changeset so I could try to port it to traefik 1.x. Is it included in golang libraries and we'd only need to rebuild 1.x or there's some actual handling somewhere in the code?

svx 11 October 16, 2023, 1:32pm

Hi @Jancis , thanks for your interest in Traefik!

You can find the PR with the related changes on **GitHub**.

As a reminder, Traefik is EOL, you can find more information about supported versions on the **release overview page**.

Related topics

Topic	Replies	Activity
Vulnerability for v2.10.7 docker	7	April 30, 2024
Potential CVEs in v2.10.7 file	4	May 15, 2024
New Security Updates for Traefik 2.10 and 3.0.0-beta	2	October 19, 2023
Several CVE's present on the latest traefik version	1	November 1, 2023

Topic	Replies	Activity
New Security Updates for Traefik 2.10 (2.10.6) and 3.0 (3.0.0-beta5)	0	December 4, 2023