CERT-EU

Security Advisory 2024-102

Traefik Critical Vulnerability

September 24, 2024 — v1.0

TLP:CLEAR

History:

- *24/09/2024 — v1.0 – Initial publication*

Summary

On September 19, 2024, a security advisory was issued regarding a critical vulnerability, **CVE-2024-45410**, affecting Traefik. This vulnerability could allow an attacker to execute arbitrary commands via crafted HTTP requests, posing a significant risk to exposed services [1,2].

Immediate updates are recommended for all affected installations.

Technical Details

The vulnerability **CVE-2024-45410** has a CVSS score of 9.8 out of 10. It allows remote code execution due to improper validation of input.

The vulnerability arises from Traefik's handling of HTTP headers which are added during request processing. It was found that certain custom headers could be removed or manipulated due to HTTP/1.1 behaviour allowing hop-by-hop headers via the Connection header. There are no known workarounds [1,2].

Affected Products

- Traefik versions prior to **2.11.9** and **3.1.3** [3,4]

Recommendations

CERT-EU strongly recommends updating as soon as possible to mitigate the risk of exploitation.

References

[1] https://github.com/traefik/traefik/security/advisories/GHSA-62c8-mh53-4cqv

[2] https://nvd.nist.gov/vuln/detail/CVE-2024-45410

[3] https://github.com/traefik/traefik/releases/tag/v3.1.3

[4] https://github.com/traefik/traefik/releases/tag/v2.11.9