

[aio-lib/aiohttp](#) Public[Code](#) [Issues](#) 185 [Pull requests](#) 91 [Discussions](#) [Actions](#) [Security an](#)

Uncapped memory usage possible via headers/trailers

Moderate [Dreamsorcerer](#) published [GHSA-w2fm-2cpv-w7v5](#) 4 days ago

Package

 [aiohttp](#) (pip)

Affected versions

<=3.13.3

Patched versions

3.13.4

Description

Summary

Insufficient restrictions in header/trailer handling could cause uncapped memory usage.

Impact

An application could cause memory exhaustion when receiving an attacker controlled request or response. A vulnerable web application could mitigate these risks with a typical reverse proxy configuration.

Patch: [0c2e9da](#)

Severity

Moderate

CVE ID

CVE-2026-22815

Weaknesses

- ▶ CWE-400
- ▶ CWE-770

Credits

 **sg3-141-592**

Reporter

 **Dreamsorcerer**

Remediation developer