# Multipart Header Size Bypass

Low **Dreamsorcerer** published **GHSA-m5qp-6w8w-w647** 20 hours ago

**Package**

**aiohttp** (pip)

**Affected versions**

<=3.13.3

**Patched versions**

3.13.4

**Description**

## Summary

A response with an excessive number of multipart headers may be allowed to use more memory than intended, potentially allowing a DoS vulnerability.

## Impact

Multipart headers were not subject to the same size restrictions in place for normal headers, potentially allowing substantially more data to be loaded into memory than intended. However, other restrictions in place limit the impact of this vulnerability.

---

Patch: `8a74257`

**Severity**

Low

**CVE ID**

CVE-2026-34516

**Weaknesses**

No CWEs

### Credits

**bekkaze** Reporter



**Dreamsorcerer** Remediation developer