EEF-CVE-2026-32145

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-32145.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-32145.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-32145
Aliases	CVE-2026-32145 GHSA-8645-p2v4-73r2
Published	2026-04-02T10:30:47.485Z
Modified	2026-04-07T04:07:10.339Z
Severity	8.7 (High) CVSS_V4 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N CVSS Calculator

Summary

Multipart form body parser bypasses body size limits in wisp

Details

Allocation of Resources Without Limits or Throttling vulnerability in gleam-wisp wisp allows a denial of service via multipart form body parsing.

The multipart*body function bypasses configured max*body*size and max*files*size limits. When a multipart boundary is not present in a chunk, the parser takes the MoreRequiredForBody path, which appends the chunk to the output but passes the quota unchanged to the recursive call. Only the final chunk containing the boundary is counted via decrement*quota. The same pattern exists in multipart*headers, where MoreRequiredForHeaders recurses without calling decrement*body_quota.

An unauthenticated attacker can exhaust server memory or disk by sending arbitrarily large multipart form submissions in a single HTTP request.

This issue affects wisp: from 0.2.0 before 2.2.2.

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:gleam-wisp:wisp:*:*:*:*:*:*:*:*"
    ],
```

```
        "capec_ids": [
            "CAPEC-130"
        ],
        "cwe_ids": [
            "CWE-770"
        ]
    }
```


References

https://github.com/gleam-wisp/wisp/security/advisories/GHSA-8645-p2v4-73r2

https://cna.erlef.org/cves/CVE-2026-32145.html

https://github.com/gleam-wisp/wisp/commit/7a978748e12ab29db232c222254465890e1a4a90

https://hex.pm/packages/wisp

Credits

John Downey - FINDER

Louis Pilfold - REMEDIATION_DEVELOPER

Affected packages

Hex
wisp

Git
github.com/gleam-wisp/wisp.git

Package

Name wisp

Purl pkg:hex/wisp

Affected ranges

Type SEMVER

Events Introduced
0.2.0
Fixed
2.2.2

Affected versions

- 0.*
- 1.*

- 2.*

Database specific

- source
