EEF-CVE-2026-42788

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

Source	https://cna.erlef.org/osv/EEF-CVE-2026-42788.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-42788.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-42788
Aliases	CVE-2026-42788 GHSA-q6v9-r226-v65f
Published	2026-05-01T20:34:11.911Z
Modified	2026-05-01T20:56:32.918100594Z
Severity	6.9 (Medium) CVSS_V4 - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N CVSS Calculator
Summary	HTTP/2 frame size limit checked after body is buffered in bandit
Details	

Summary

Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated memory exhaustion via oversized HTTP/2 frames.

'Elixir.Bandit.HTTP2.Frame':deserialize/2 in lib/bandit/http2/frame.ex checks the SETTINGS*MAX*FRAME*SIZE limit only after pattern-matching payload::binary-size(length), which requires the entire frame body to be present in memory before either the accept or reject clause can fire. A peer that announces a frame length up to the 24-bit maximum (~16 MiB) causes the server to buffer that entire body before the size guard is evaluated, regardless of the max*frame_size negotiated during the HTTP/2 handshake (default 16 KiB per RFC 9113).

An unauthenticated attacker holding many concurrent connections can force the server to buffer far more memory than the negotiated frame size limit should permit, leading to memory pressure and potential denial of service.

This issue affects bandit: from 0.3.6 before 1.11.0.

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:mtrudel:bandit:*:*:*:*:*:*:*:*"
    ],
    "cwe_ids": [
        "CWE-770"
    ],
    "capec_ids": [
        "CAPEC-130"
    ]
}
```


References

https://github.com/mtrudel/bandit/security/advisories/GHSA-q6v9-r226-v65f

https://cna.erlef.org/cves/CVE-2026-42788.html

https://github.com/mtrudel/bandit/commit/1e8e55966da9129016b73d32f0e1df4630e3b463

https://hex.pm/packages/bandit

Credits

Peter Ullrich - FINDER

Mat Trudel - REMEDIATION_DEVELOPER

Jonatan Männchen - ANALYST

Affected packages

Hex
bandit

Git
github.com/mtrudel/bandit

Package

Name bandit

Purl pkg:hex/bandit

Affected ranges

Type SEMVER

Events Introduced
0.3.6
Fixed

1.11.0

Affected versions

- 0.*
- 1.*

Database specific

- source