CVE-2026-42788

HTTP/2 frame size limit checked after body is buffered in bandit

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-770 — CWE-770 Allocation of Resources Without Limits or Throttling

CAPEC

CAPEC-130 — CAPEC-130 Excessive Allocation

CVSS 4.0 Score

6.9

MEDIUM

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

Vulnerability description

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.

Affected

pkg:hex/bandit

Module	Source File	Routine
Bandit.HTTP2.Frame	lib/bandit/http2/frame.ex	Bandit.HTTP2.Frame.deserialize/2

Status	Type	Version	Changes / Fixed in
Affected	semver ⓘ	0.3.6	< 1.11.0

pkg:github/mtrudel/bandit

Module	Source File	Routine
Bandit.HTTP2.Frame	lib/bandit/http2/frame.ex	Bandit.HTTP2.Frame.deserialize/2

Status	Type	Version	Changes / Fixed in
Affected	git ⓘ	f00dd69a5b	< 1.11.0

References

- https://github.com/mtrudel/bandit/security/advisories/GHSA-q6v9-r226-v65f **vendor-advisory** **related**
- https://osv.dev/vulnerability/EEF-CVE-2026-42788 **related**
- https://github.com/mtrudel/bandit/commit/1e8e55966da9129016b73d32f0e1df4630e3b463 **patch**

Credits

- **Finder**: Peter Ullrich
- **Remediation developer**: Mat Trudel
- **Analyst**: Jonatan Männchen

CVE record as JSON: `GET /cves/CVE-2026-42788.json`
OSV record as JSON: `GET /osv/EEF-CVE-2026-42788.json`