

CVE-2026-39804

WebSocket permessage-deflate inflate has no output-size cap 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

8.2

HIGH

[CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N](#)

Vulnerability description

Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated remote denial of service via memory exhaustion when WebSocket permessage-deflate compression is enabled.

'Elixir.Bandit.WebSocket.PerMessageDeflate':inflate/2 in lib/bandit/websocket/permessage_deflate.ex calls :zlib.inflate/2 with no output-size cap, then materializes the entire decompressed payload as a single binary via IO.iodata_to_binary/1. The websocket_options.max_frame_size option only bounds the on-the-wire (compressed) frame size, not the decompressed output. A high-ratio compressed frame (e.g. uniform data at ~1024:1 ratio) can stay well under any wire-size limit while forcing GiB-scale heap allocations in the connection process before any application code runs.

An unauthenticated attacker who can open a WebSocket connection can send a single such frame to exhaust the BEAM node's memory and trigger an OOM kill.

This vulnerability requires both Bandit's server-level websocket_options.compress and the per-upgrade compress: true option passed to WebSockAdapter.upgrade/4 to be enabled. Stock Phoenix and LiveView applications are not affected as they default to compress: false.

This issue affects bandit: from 0.5.9 before 1.11.0.


Affected

[pkg:hex/bandit](#)

Module	Source File	Routine	
Bandit.WebSocket.PerMessageDeflate	lib/bandit/websocket/permessage_deflate.ex	Bandit.WebSocket.PerMessageDeflate.i	
Status	Type	Version	Changes / Fixed in
Affected	semver i	0.5.9	< 1.11.0

[pkg:github/mtrudel/bandit](#)

Module	Source File	Routine
Bandit.WebSocket.PerMessageDeflate	lib/bandit/websocket/permessage_deflate.ex	Bandit.WebSocket.PerMessageDeflate.i

Status	Type	Version	Changes / Fixed in
Affected	git 	da4027cff7	< 1.11.0

Configurations

The vulnerability is only reachable when both of the following conditions are true:

- Bandit's server-level `websocket_options.compress` is enabled (it defaults to `true`).
- The per-upgrade `compress: true` option is passed to `WebSockAdapter.upgrade/4` (it defaults to `false`; Phoenix's default is also `false`).

Stock Phoenix and LiveView applications are not affected because `compress: false` is their default.

Workarounds

Do not pass `compress: true` to `WebSockAdapter.upgrade/4`. Omitting this option (or setting it to `false`) prevents `permessage-deflate` from being negotiated, so the `inflate` path is never reached.

References

- <https://github.com/mtrudel/bandit/security/advisories/GHSA-frh3-6pv6-rc8j> vendor-advisory related
- <https://osv.dev/vulnerability/EEF-CVE-2026-39804> related
- <https://github.com/mtrudel/bandit/commit/8156921a51e684a951221da7bc30a70a022f722e> patch

Credits

- Finder:** Peter Ullrich

CVE record as JSON: <GET /cves/CVE-2026-39804.json>

OSV record as JSON: <GET /osv/EEF-CVE-2026-39804.json>



ERLANG ECOSYSTEM
FOUNDATION

Supporting the BEAM community

ABOUT THE EEF

[Membership details](#)

[Join us!](#)

[Sponsors](#)

[Working Groups](#)

[Stipends](#)

[Bylaws](#)

[FAQ](#)

STAY UP-TO-DATE

[News](#)

[Events](#)

GET IN TOUCH

[Contact Us](#)