EEF-CVE-2026-39804

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

Source	https://cna.erlef.org/osv/EEF-CVE-2026-39804.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-39804.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-39804
Aliases	CVE-2026-39804 GHSA-frh3-6pv6-rc8j
Published	2026-05-01T20:34:24.604Z
Modified	2026-05-01T20:56:32.721220593Z
Severity	8.2 (High) CVSS_V4 – 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 CVSS Calculator
Summary	WebSocket permessage-deflate inflate has no output-size cap in bandit
Details	

Summary

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.

Workaround

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.

Configuration

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.

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-frh3-6pv6-rc8j

https://cna.erlef.org/cves/CVE-2026-39804.html

https://github.com/mtrudel/bandit/commit/8156921a51e684a951221da7bc30a70a022f722e

https://hex.pm/packages/bandit

Credits

Peter Ullrich - FINDER

Affected packages

Hex
bandit

Git
github.com/mtrudel/bandit

Package

Name bandit

Purl pkg:hex/bandit

Affected ranges

Type SEMVER

Events Introduced
0.5.9
Fixed
1.11.0

Affected versions

▸ 0.*

▸ 1.*

Database specific

▸ source