

CVE-2026-42786

WebSocket fragmented message reassembly unbounded 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

8.7

HIGH
[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](#)

Vulnerability description

Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated remote denial of service via memory exhaustion.

The fragment reassembly path in `'Elixir.Bandit.WebSocket.Connection':handle_frame/3` in `lib/bandit/websocket/connection.ex` appends every incoming `Continuation{fin: false}` frame's payload to a per-connection iolist with no cumulative size cap. The existing `max_frame_size` option only bounds individual frames; a peer that streams an unbounded number of continuation frames without ever setting `fin=1` grows BEAM heap linearly until the OS or a supervisor kills the process.

Because the accumulation happens before `WebSock.handle_in/2` is called, the application has no opportunity to interpose a size check. Phoenix Channels and LiveView both run over `WebSock` on Bandit, so a stock Phoenix application exposes this surface as soon as it accepts socket connections.

This issue affects bandit: from 0.5.0 before 1.11.0.

Affected

[pkg:hex/bandit](#)

| Module | Source File | Routine | |
|---|--|--|--------------------------|
| Bandit.WebSocket.Connection | lib/bandit/websocket/connection.ex | Bandit.WebSocket.Connection.handle_frame/3 | |
| Status | Type | Version | Changes / Fixed in |
| Affected | semver 📄 | 0.5.0 | < 1.11.0 |

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

| Module | Source File | Routine | |
|--|--|---|--------------------------|
| <code>Bandit.WebSocket.Connection</code> | lib/bandit/websocket/connection.ex | <code>Bandit.WebSocket.Connection.handle_frame/3</code> | |
| Status | Type | Version | Changes / Fixed in |
| Affected | git 📄 | 8909391f48 | < 1.11.0 |

Configurations

The application must accept WebSocket connections. Applications that expose no WebSocket endpoints are not affected.

References

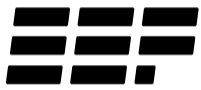
- <https://github.com/mtrudel/bandit/security/advisories/GHSA-pf94-94m9-536p> vendor-advisory related
- <https://osv.dev/vulnerability/EEF-CVE-2026-42786> related
- <https://github.com/mtrudel/bandit/commit/21612c7c7b1ce43eccd36d3af3a2299d23513667> patch

Credits

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

CVE record as JSON: [GET /cves/CVE-2026-42786.json](https://cves.cve.org/cves/CVE-2026-42786.json)

OSV record as JSON: [GET /osv/EEF-CVE-2026-42786.json](https://osv.dev/EEF-CVE-2026-42786.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](#)

