



Vulnerability  
Database

Blog

FAQ  
[↗](#)

Docs  
[↗](#)



# EEF-CVE- 2026-42786

[See a problem?](#)

Please try reporting it [to the source](#) [↗](#) first.

Source	<a href="https://cna.erlef.org/osv/EEF-CVE-2026-42786.html">https://cna.erlef.org/osv/EEF-CVE-2026-42786.html</a> <a href="#">↗</a>
Import Source	<a href="https://cna.erlef.org/osv/EEF-CVE-2026-42786.json">https://cna.erlef.org/osv/EEF-CVE-2026-42786.json</a> <a href="#">↗</a>
JSON Data	<a href="https://api.osv.dev/v1/vulns/EEF-CVE-2026-42786">https://api.osv.dev/v1/vulns/EEF-CVE-2026-42786</a> <a href="#">↗</a>
Aliases	CVE-2026-42786 GHSA-pf94-94m9-536p
Published	2026-05-01T20:34:17.014Z
Modified	2026-05-02T04:17:26.677Z
Severity	<b>8.7 (High)</b> CVSS_V4 - 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 <a href="#">CVSS Calculator</a> <a href="#">↗</a>

**Summary** WebSocket fragmented message reassembly unbounded in bandit

**Details**

## Summary

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':handleframe/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 `maxframe_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.

## Configuration

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

**Database specific** [↗](#)

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

### References

<https://github.com/mtrudel/bandit/security/advisories/GHSA-pf94-94m9-536p> [↗](#)

<https://cna.erlef.org/cves/CVE-2026-42786.html> [↗](#)

<https://github.com/mtrudel/bandit/commit/21612c7c7b1ce43eccd36d3af3a2299d23513667> [↗](#)

<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  
0.5.0  
Fixed  
1.11.0

---

### Affected versions [↗](#)

▶ 0.\*

▶ 1.\*

---

### Database specific [↗](#)

▶ source

---