



Vulnerability
Database

Blog

FAQ
[↗](#)

Docs
[↗](#)



EEF-CVE- 2026-39805

[See a problem?](#)

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

Source	https://cna.erlef.org/osv/EEF-CVE-2026-39805.html ↗
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-39805.json ↗
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-39805 ↗
Aliases	CVE-2026-39805 GHSA-c67r-gc9j-2qf7
Published	2026-05-01T20:34:29.400Z
Modified	2026-05-01T20:56:32.572885294Z
Severity	6.3 (Medium) CVSS_V4 - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N CVSS Calculator ↗

Summary CL.CL HTTP request smuggling via duplicate Content-Length in bandit

Details

Summary

Inconsistent Interpretation of HTTP Requests vulnerability in mtrudel bandit allows HTTP request smuggling via duplicate Content-Length headers.

'Elixir.Bandit.Headers':getcontentlength/1 in lib/bandit/headers.ex uses List.keyfind/3, which returns only the first matching header. When a request contains two Content-Length headers with different values, Bandit silently accepts it, uses the first value to read the body, and dispatches the remaining bytes as a second pipelined request on the same keep-alive connection. RFC 9112 §6.3 requires recipients to treat this as an unrecoverable framing error.

When Bandit sits behind a proxy that picks the last Content-Length value and forwards the request rather than rejecting it, an unauthenticated attacker can smuggle requests past edge WAF rules, path-based ACLs, rate limiting, and audit logging.

This issue affects bandit: before 1.11.0.

Database specific [↗](#) {

```
"cpe_ids": [
  "cpe:2.3:a:mtrudel:bandit:*:*:*:*:*:*:*:*"
],
"capec_ids": [
  "CAPEC-33"
],
"cwe_ids": [
  "CWE-444"
]
}
```

References

<https://github.com/mtrudel/bandit/security/advisories/GHSA-c67r-gc9j-2qf7> [↗](#)

<https://cna.erlef.org/cves/CVE-2026-39805.html> [↗](#)

<https://github.com/mtrudel/bandit/commit/f2ca636eb6df385219957e8934e9fc6efa1630d1> [↗](#)

<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
	Fixed
	1.11.0

Affected versions [↗](#)

▶ 0.*

▶ 1.*

Database specific [↗](#)

▶ source
