CVE-2026-39805

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

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-444 — CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

CAPEC

CAPEC-33 — CAPEC-33 HTTP Request Smuggling

CVSS 4.0 Score

6.3

MEDIUM

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

Vulnerability description

Inconsistent Interpretation of HTTP Requests vulnerability in mtrudel bandit allows HTTP request smuggling via duplicate `Content-Length` headers.
`'Elixir.Bandit.Headers':get_content_length/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.

Affected

pkg:hex/bandit

Module	Source File	Routine
Bandit.Headers	lib/bandit/headers.ex	Bandit.Headers.get_content_length/1

Status	Type	Version	Changes / Fixed in
Affected	semver ⓘ	initial	< 1.11.0

pkg:github/mtrudel/bandit

Module	Source File	Routine
Bandit.Headers	lib/bandit/headers.ex	Bandit.Headers.get_content_length/1

Status	Type	Version	Changes / Fixed in
Affected	git ⓘ	initial	< 1.11.0

References

- https://github.com/mtrudel/bandit/security/advisories/GHSA-c67r-gc9j-2qf7 vendor-advisory related

- https://osv.dev/vulnerability/EEF-CVE-2026-39805 related
- https://github.com/mtrudel/bandit/commit/f2ca636eb6df385219957e8934e9fc6efa1630d1 patch

Credits

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

CVE record as JSON: `GET /cves/CVE-2026-39805.json`
OSV record as JSON: `GET /osv/EEF-CVE-2026-39805.json`
