CVE-2026-39807

Client-supplied URI scheme trusted without transport verification in bandit

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-807 — CWE-807 Reliance on Untrusted Inputs in a Security Decision

CAPEC

CAPEC-220 — CAPEC-220 Client-Server Protocol Manipulation

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

Reliance on Untrusted Inputs in a Security Decision vulnerability in mtrudel bandit allows unauthenticated transport-state spoofing on plaintext HTTP connections.
`'Elixir.Bandit.Pipeline':determine_scheme/2` in `lib/bandit/pipeline.ex` returns the client-supplied URI scheme verbatim, ignoring the transport's `secure?` flag. HTTP/1.1 absolute-form request targets (e.g. `GET https://victim/path HTTP/1.1`) and the HTTP/2 `:scheme` pseudo-header are both attacker-controlled strings that flow through this function. Over a plaintext TCP connection, a client can declare `https` and Bandit will set `conn.scheme = :https` even though no TLS was negotiated.

Downstream Plug consumers that branch on `conn.scheme` are silently misled: `Plug.SSL`'s already-secure branch skips its HTTP→HTTPS redirect, cookies emitted with `secure: true` are sent over plaintext, audit logs record requests as having arrived over HTTPS, and CSRF/SameSite gating may make incorrect decisions.

This issue affects bandit: from 1.0.0 before 1.11.0.

Affected

pkg:hex/bandit

Module	Source File	Routine
Bandit.Pipeline	lib/bandit/pipeline.ex	Bandit.Pipeline.determine_scheme/2

Status	Type	Version	Changes / Fixed in
Affected	semver ⓘ	1.0.0	< 1.11.0

pkg:github/mtrudel/bandit

Module	Source File	Routine
Bandit.Pipeline	lib/bandit/pipeline.ex	Bandit.Pipeline.determine_scheme/2

Status	Type	Version	Changes / Fixed in
Affected	git ⓘ	ff2f829326	< 1.11.0

Configurations

The vulnerable system must be accepting plaintext (non-TLS) HTTP connections, either directly or via h2c. Deployments that exclusively use TLS are not affected.

References

- https://github.com/mtrudel/bandit/security/advisories/GHSA-375f-4r2h-f99j vendor-advisory related
- https://osv.dev/vulnerability/EEF-CVE-2026-39807 related
- https://github.com/mtrudel/bandit/commit/45feea20dea8af7ffd7245271107b695c040e667 patch

Credits

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

CVE record as JSON: `GET /cves/CVE-2026-39807.json`
OSV record as JSON: `GET /osv/EEF-CVE-2026-39807.json`