EEF-CVE-2026-39807

See a problem? Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-39807.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-39807.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-39807
Aliases	CVE-2026-39807 GHSA-375f-4r2h-f99j
Published	2026-05-01T20:34:22.832Z
Modified	2026-05-01T20:56:32.836978922Z
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	Client-supplied URI scheme trusted without transport verification in bandit

Details

Summary

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.

Configuration

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

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:mtrudel:bandit:*:*:*:*:*:*:*:*"
    ],
    "capec_ids": [
        "CAPEC-220"
    ],
    "cwe_ids": [
        "CWE-807"
    ]
}
```


References

https://github.com/mtrudel/bandit/security/advisories/GHSA-375f-4r2h-f99j

https://cna.erlef.org/cves/CVE-2026-39807.html

https://github.com/mtrudel/bandit/commit/45feea20dea8af7ffd7245271107b695c040e667

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
1.0.0
Fixed
1.11.0

Affected versions

▸ 1.*

Database specific

▸ source