CVE-2026-28808

ScriptAlias CGI targets bypass directory auth in inets httpd (mod_auth vs mod_cgi path mismatch)

« Back to all CVEs

See on OSV.dev »

Weakness Type (CWE)

CWE-863 — CWE-863 Incorrect Authorization

CAPEC

CAPEC-1 — CAPEC-1 Accessing Functionality Not Properly Constrained by ACLs

CVSS 4.0 Score

8.3

HIGH

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

Vulnerability description

Incorrect Authorization vulnerability in Erlang OTP (inets modules) allows unauthenticated access to CGI scripts protected by `directory` rules when served via `script_alias`.
When `script_alias` maps a URL prefix to a directory outside `DocumentRoot`, `mod_auth` evaluates `directory`-based access controls against the `DocumentRoot`-relative path while `mod_cgi` executes the script at the `ScriptAlias`-resolved path. This path mismatch allows unauthenticated access to CGI scripts that `directory` rules were meant to protect.

This vulnerability is associated with program files `lib/inets/src/http_server/mod_alias.erl`, `lib/inets/src/http_server/mod_auth.erl`, and `lib/inets/src/http_server/mod_cgi.erl`.

This issue affects OTP from OTP 17.0 until OTP 28.4.2, 27.3.4.10 and 26.2.5.19 corresponding to inets from 5.10 until 9.6.2, 9.3.2.4 and 9.1.0.6.

Affected

`pkg:otp/inets`

Module	Source File
inets	src/http_server/mod_alias.erl
	src/http_server/mod_auth.erl
	src/http_server/mod_cgi.erl

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	5.10	• unaffected at 9.6.2 • unaffected at 9.3.2.4 • unaffected at 9.1.0.6

pkg:github/erlang/otp

Module	Source File
inets	lib/inets/src/http_server/mod_alias.erl

Module	Source File
	lib/inets/src/http_server/mod_auth.erl
	lib/inets/src/http_server/mod_cgi.erl

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	17.0	• unaffected at 28.4.2 • unaffected at 27.3.4.10 • unaffected at 26.2.5.19
Affected	git ⓘ	07b8f441ca	• unaffected at 8fc71ac6af • unaffected at 9dfa0c51ea

Configurations

The inets httpd server must use `script_alias` to map a URL prefix to a CGI directory, combined with `directory`-based access controls (e.g., `mod_auth`) protecting the `script_alias` target path. The vulnerability applies whenever the `script_alias` target path differs from `DocumentRoot` + URL prefix.

Workarounds

- Move CGI scripts inside `DocumentRoot` and use `alias` instead of `script_alias` to ensure `mod_auth` resolves the correct path.
- Apply URL-based access controls at a reverse proxy layer to block unauthenticated access to the `script_alias` URL prefix.
- Remove `mod_cgi` from the httpd modules chain if CGI functionality is not required.

References

- https://github.com/erlang/otp/security/advisories/GHSA-3vhp-h532-mc3f vendor-advisory related
- https://osv.dev/vulnerability/EEF-CVE-2026-28808 related
- https://github.com/erlang/otp/commit/8fc71ac6af4fbcc54103bec2983ef22e82942688 patch
- https://github.com/erlang/otp/commit/9dfa0c51eac97866078e808dec2183cb7871ff7c patch

Credits

- **Reporter**: Igor Morgenstern / Aisle Research
- **Remediation developer**: Konrad Pietrzak

CVE record as JSON: GET /cves/CVE-2026-28808.json
OSV record as JSON: GET /osv/EEF-CVE-2026-28808.json