



EEF-CVE- 2026-28808

[See a problem?](#)

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

Source	https://cna.erlef.org/osv/EEF-CVE-2026-28808.html ↗
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-28808.json ↗
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-28808 ↗
Aliases	CVE-2026-28808 GHSA-3vhp-h532-mc3f
Published	2026-04-07T12:28:16.056Z
Modified	2026-04-07T15:00:15.886464Z
Severity	8.3 (High) CVSS_V4 - 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 CVSS Calculator ↗

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

Details

Summary

Incorrect Authorization vulnerability in Erlang OTP (inets modules) allows unauthenticated access to CGI scripts protected by directory rules when served via script_alias.

When *scriptalias* maps a URL prefix to a directory outside *DocumentRoot*, *modauth* 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/httpserver/modalias.erl`, `lib/inets/src/httpserver/modauth.erl`, and
`lib/inets/src/httpserver/modcgi.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.

Workaround

- Move CGI scripts inside DocumentRoot and use alias instead of scriptalias to ensure modauth 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.

Configuration

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

Database specific  {

```
  "cpe_ids": [
    "cpe:2.3:a:erlang:erlang\\/otp:*:*:*:*:*:*:*:*"
  ],
  "capec_ids": [
    "CAPEC-1"
  ],
  "cwe_ids": [
    "CWE-863"
  ]
}
```


References

<https://github.com/erlang/otp/security/advisories/GHSA-3vhp-h532-mc3f> 

<https://cna.erlef.org/cves/CVE-2026-28808.html> 

<https://www.erlang.org/doc/system/versions.html#order-of-versions> 

<https://github.com/erlang/otp/commit/8fc71ac6af4fbcc54103bec2983ef22e82942688> 

<https://github.com/erlang/otp/commit/9dfa0c51eac97866078e808dec2183cb7871ff7c> 

Credits

Igor Morgenstern / Aisle Research - REPORTER

Konrad Pietrzak - REMEDIATION_DEVELOPER

Affected packages

Git
github.com/erlang/otp

Affected ranges [↗](#)

Type GIT

Repo <https://github.com/erlang/otp>

Events Introduced

[07b8f441ca711f9812fad9e9115bab3c3aa92f79](#) [↗](#)

Fixed

[8fc71ac6af4fbcc54103bec2983ef22e82942688](#) [↗](#)

Fixed

[9dfa0c51eac97866078e808dec2183cb7871ff7c](#) [↗](#)

Affected versions [↗](#)

▶ OTP-17.*

▶ OTP-18.*

▶ OTP-19.*

▶ OTP-20.*

▶ OTP-21.*

▶ OTP-22.*

▶ OTP-23.*

▶ OTP-24.*

▶ OTP-25.*

▶ OTP-26.*

▶ OTP-27.*

▶ OTP-28.*

▶ OTP-29.*

▶ Other

Database specific [↗](#)

▶ source
