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

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-28808 |
| **State** | PUBLISHED |
| **Assigner** | EEF |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-07 13:16:46 UTC |
| **Updated** | 2026-04-07 13:20:11 UTC |
| **Description** | Incorrect Authorization vulnerability in Erlang OTP (inets modules) allows unauthenticated access to CGI scripts protected b |

## Risk And Classification

**Primary CVSS:** v4.0 8.3 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-863 | CWE-863 CWE-863 Incorrect Authorization

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | Secondary | 8.3 | HIGH | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N |
| 4.0 | CNA | CVSS | 8.3 | HIGH | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Erlang | OTP | affected 5.10 * otp | Not specified |
| CNA | Erlang | OTP | affected 17.0 * otp | Not specified |
| CNA | Erlang | OTP | affected 07b8f441ca711f9812fad9e9115bab3c3aa92f79 * git | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| cna.erlef.org/cves/CVE-2026-28808.html | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | cna.erlef.org |
| github.com/erlang/otp/commit/9dfa0c51eac97866078e808dec2183cb7871ff7c | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| www.erlang.org/doc/system/versions.html | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | www.erlang.org |
| osv.dev/vulnerability/EEF-CVE-2026-28808 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | osv.dev |
| github.com/erlang/otp/security/advisories/GHSA-3vhp-h532-mc3f | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| github.com/erlang/otp/commit/8fc71ac6af4fbcc54103bec2983ef22e82942688 | 6b3ad84c-e1a6-4bf7-a703-f496b71e49db | github.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Igor Morgenstern / Aisle Research (en)

**CNA:** Konrad Pietrzak (en)

## Additional Advisory Data

Workarounds

**CNA:** * 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.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**