# ScriptAlias CGI targets bypass `directory` auth (mod_auth vs mod_cgi path mismatch)

High **Whaileee** published **GHSA-3vhp-h532-mc3f** 2 weeks ago

**Package**

**OTP**

| Affected versions | Patched versions |
| --- | --- |
| >= 17.0 | 28.4.2, 27.3.4.10, 26.2.5.19 |

**inets** (OTP)

| | |
| --- | --- |
| >= 5.10 | 9.1.0.6, 9.3.2.4, 9.6.2 |

**Description**

## Impact

The Erlang/OTP `inets` HTTP server (`httpd`) is vulnerable to an authentication bypass when `script_alias` is used to map a URL prefix to a CGI script directory located outside `DocumentRoot`, and directory-based access controls (`mod_auth`) are configured to protect that directory.

The `mod_alias` module fails to include `script_alias` entries when resolving request paths. This causes `mod_auth` to evaluate authorization rules against an incorrect `DocumentRoot`-relative path, while `mod_cgi` independently resolves and executes the script at the correct `script_alias` target path — without authentication.

**You are affected if all of the following apply:**

- You use the Erlang/OTP `inets` HTTP server (`httpd`)
- You have configured `script_alias` mapping a URL prefix to a directory **outside** `DocumentRoot`
- You have configured `mod_auth` directory-based access controls to protect that external directory

**You are NOT affected if:**

- You do not use `script_alias`, or your `script_alias` targets reside inside `DocumentRoot`
- You use `erl_script_alias` (`mod_esi`) instead — it maps to Erlang modules, not filesystem paths
- You do not use `mod_auth` directory-based access controls on `script_alias` targets
- You use an external reverse proxy for authentication enforcement

## 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

## Affected/Unaffected Versions

A version larger than or equal to one of the listed *patched versions* is **unaffected**; *otherwise*, a version that satisfies an expression listed under *affected versions* is **affected**, and if it does not, it is **unaffected**.

The documentation of the new *OTP version scheme* describes how versions should be compared. Note that versions used prior to OTP 17.0, when the new *OTP version scheme* was introduced, are never listed since it is not well defined how to compare those versions.

In the case of this vulnerability, versions prior to OTP 17.0 are likely also affected.

## Credits

Thanks to (imorgenstern) for finding and responsibly disclosing this vulnerability to the Erlang/OTP project.

**Severity**

High 8.3 / 10

**CVSS v4 base metrics**

**Exploitability Metrics**

| | |
|---|---|
| Attack Vector | Network |
| Attack Complexity | Low |
| Attack Requirements | Present |
| Privileges Required | None |
| User interaction | None |

**Vulnerable System Impact Metrics**

| | |
|---|---|
| Confidentiality | High |
| Integrity | Low |
| Availability | None |
| **Subsequent System Impact Metrics** | |
| Confidentiality | None |
| Integrity | None |
| Availability | None |

Learn more about base metrics

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

### CVE ID

CVE-2026-28808

### Weaknesses

▶ CWE-863

### Credits

**imorgenstern** Reporter