EEF-CVE-2025-4748

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

Source	https://cna.erlef.org/osv/EEF-CVE-2025-4748.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2025-4748.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2025-4748
Aliases	CVE-2025-4748 GHSA-9g37-pgj9-wrhc
Published	2025-06-16T11:00:54.643Z
Modified	2026-04-06T17:01:59.863466Z
Severity	4.8 (Medium) CVSS_V4 - CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L/SC:N/SI:L/SA:L CVSS Calculator
Summary	Absolute path traversal in zip:unzip/1,2
Details	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP (stdlib modules) allows Absolute Path Traversal, File Manipulation. This vulnerability is associated with program files lib/stdlib/src/zip.erl and program routines zip:unzip/1, zip:unzip/2, zip:extract/1, zip:extract/2 unless the memory option is passed. This issue affects OTP from OTP 17.0 until OTP 28.0.1, OTP 27.3.4.1 and OTP 26.2.5.13, corresponding to stdlib from 2.0 until 7.0.1, 6.2.2.1 and 5.2.3.4.

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:erlang:erlang\\/otp:*:*:*:*:*:*:*:*"
    ],
    "cwe_ids": [
        "CWE-22"
    ],
    "capec_ids": [
        "CAPEC-597",
        "CAPEC-165"
```

```
        ]
    }
```


References

https://github.com/erlang/otp/security/advisories/GHSA-9g37-pgj9-wrhc

https://cna.erlef.org/cves/CVE-2025-4748.html

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

https://github.com/erlang/otp/pull/9941

https://github.com/erlang/otp/commit/5a55feec10c9b69189d56723d8f237afa58d5d4f

https://github.com/erlang/otp/commit/ba2f2bc5f45fcfd2d6201ba07990a678bbf4cc8f

https://github.com/erlang/otp/commit/578d4001575aa7647ea1efd4b2b7e3afadcc99a5

Credits

Wander Nauta - FINDER

Lukas Backström - REMEDIATION_DEVELOPER

Björn Gustavsson - REMEDIATION_REVIEWER

Affected packages

Git
github.com/erlang/otp

Affected ranges

Type GIT

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

Events Introduced
07b8f441ca711f9812fad9e9115bab3c3aa92f79
Fixed
d9454dbccbaaad4b8796095c8e653b71b066dfaf
Fixed
9b7b5431260e05a16eec3ecd530a232d0995d932
Fixed
0ac548b57c0491196c27e39518b5f6acf9326c1e

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.*
- Other

Database specific

- source
