

CVE-2025-4748

# Absolute path traversal in zip:unzip/1,2

[« Back to all CVEs](#)[See on OSV.dev »](#)

## Weakness Type (CWE)

[CWE-22 — CWE-22 Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](#)

## CAPEC

[CAPEC-597 — CAPEC-597 Absolute Path Traversal](#)[CAPEC-165 — CAPEC-165 File Manipulation](#)

## CVSS 4.0 Score

# 4.8

**MEDIUM**[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](#)

## Vulnerability description

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.

## Affected

pkg:otp/stdlib

Module	Source File	Routine
<a href="#">stdlib</a>	<code>lib/stdlib/src/zip.erl</code>	<a href="#">zip:unzip/1</a> <a href="#">zip:unzip/2</a> <a href="#">zip:extract/1</a> <a href="#">zip:extract/2</a>

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	2.0	<ul style="list-style-type: none"> <li>unaffected at 7.0.1</li> <li>unaffected at 6.2.2.1</li> <li>unaffected at 5.2.3.4</li> </ul>

[pkg:github/erlang/otp](#)

Module	Source File	Routine
stdlib	<a href="#">lib/stdlib/src/zip.erl</a>	<code>zip:unzip/1</code> <code>zip:unzip/2</code> <code>zip:extract/1</code> <code>zip:extract/2</code>

Status	Type	Version	Changes / Fixed in
Affected	otp <sup>①</sup>	<a href="#">17.0</a>	<ul style="list-style-type: none"> <li>unaffected at <a href="#">28.0.1</a></li> <li>unaffected at <a href="#">27.3.4.1</a></li> <li>unaffected at <a href="#">26.2.5.13</a></li> </ul>
Affected	git <sup>①</sup>	<a href="#">07b8f441ca71</a>	<ul style="list-style-type: none"> <li>unaffected at <a href="#">d9454dbccbaa</a></li> <li>unaffected at <a href="#">9b7b5431260e</a></li> <li>unaffected at <a href="#">0ac548b57c04</a></li> </ul>

## Workarounds

You can use `zip:list_dir/1` on the archive and verify that no files contain absolute paths before extracting the archive to disk.

## References

- <https://github.com/erlang/otp/security/advisories/GHSA-9g37-pgj9-wrhc> vendor-advisory related
- <https://osv.dev/vulnerability/EEF-CVE-2025-4748> related
- <https://github.com/erlang/otp/pull/9941> patch
- <https://github.com/erlang/otp/commit/5a55feec10c9b69189d56723d8f237afa58d5d4f> patch
- <https://github.com/erlang/otp/commit/ba2f2bc5f45fcfd2d6201ba07990a678bbf4cc8f> patch
- <https://github.com/erlang/otp/commit/578d4001575aa7647ea1efd4b2b7e3afadcc99a5> patch

## Credits

- Finder:** Wander Nauta
- Remediation developer:** Lukas Backström
- Remediation reviewer:** Björn Gustavsson

CVE record as JSON: [GET /cves/CVE-2025-4748.json](#)

OSV record as JSON: [GET /osv/EEF-CVE-2025-4748.json](#)



ERLANG ECOSYSTEM  
FOUNDATION

Supporting the BEAM community

ABOUT THE EEF

[Membership details](#)

[Join us!](#)

[Sponsors](#)

[Working Groups](#)

[Stipends](#)

[Bylaws](#)

[FAQ](#)

STAY UP-TO-DATE

[News](#)

[Events](#)

GET IN TOUCH

[Contact Us](#)