Absolute path traversal in zip:unzip/1,2

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-4748
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-16 11:15:18 UTC
Updated	2026-04-06 17:17:04 UTC
Description	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP (stdlib modules) a

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

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/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-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:L

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

Low

Sub Availability

Low

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/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 2.0 * otp	Not specified
CNA	Erlang	OTP	affected 17.0 * otp	Not specified
CNA	Erlang	OTP	affected 07b8f441ca711f9812fad9e9115bab3c3aa92f79 * git	Not specified

References

Reference	Source	Link
github.com/erlang/otp/security/advisories/GHSA-9g37-pgj9-wrhc	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
www.openwall.com/lists/oss-security/2025/06/16/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.
github.com/erlang/otp/pull/9941	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2025-4748.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
github.com/erlang/otp/commit/578d4001575aa7647ea1efd4b2b7e3afadcc99a5	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/commit/ba2f2bc5f45fcfd2d6201ba07990a678bbf4cc8f	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
www.erlang.org/doc/system/versions.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	www.erlang.org
github.com/erlang/otp/commit/5a55feec10c9b69189d56723d8f237afa58d5d4f	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
osv.dev/vulnerability/EEF-CVE-2025-4748	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Wander Nauta (en)

CNA: Lukas Backström (en)

CNA: Björn Gustavsson (en)

Additional Advisory Data

Workarounds

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

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