Absolute Path in Zip Module

Moderate **IngelaAndin** published **GHSA-9g37-pgj9-wrhc** on Jun 16, 2025

Package

OTP

Affected versions	Patched versions
>= 17.0	28.0.1, 27.3.4.1, 26.2.5.13

stdlib (OTP)

>= 2.0	7.0.1, 6.2.2.1, 5.2.3.4

Description

Impact

When the zip module is used to extract files to disk and the archive is maliciously corrupted by including absolute file paths, the zip module would extract them as absolute paths instead of stripping the leading `/`, drive or device letter.

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.

Workarounds

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

Affected/Unaffected Versions

A version larger than or equal to one of the listed *patched versions* is **unaffected**; *otherwise*, a version that satisfies the 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 Wander Nauta for finding and responsibly disclosing this vulnerability to the Erlang/OTP project.

Severity

Moderate 4.8 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	Low
Availability	Low
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	Low
Availability	Low

Learn more about base metrics

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

CVE ID

CVE-2025-4748

Weaknesses

▶ CWE-22

Credits

wandernauta Reporter