CVE-2026-32147

SFTP chroot bypass via path traversal in SSH_FXP_FSETSTAT

« 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')

CVSS 4.0 Score

5.3

MEDIUM

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N

Vulnerability description

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Erlang OTP `ssh` (`ssh_sftpd` module) allows an authenticated SFTP user to modify file attributes outside the configured chroot directory.
The SFTP daemon (`ssh_sftpd`) stores the raw, user-supplied path in file handles instead of the chroot-resolved path. When `SSH_FXP_FSETSTAT` is issued on such a handle, file attributes (permissions, ownership, timestamps) are modified on the real filesystem path, bypassing the root directory boundary entirely.

Any authenticated SFTP user on a server configured with the `root` option can modify file attributes of files outside the intended chroot boundary. The prerequisite is that a target file must exist on the real filesystem at the same relative path. Note that this vulnerability only allows modification of file attributes; file contents cannot be read or altered through this attack vector.

If the SSH daemon runs as `root`, this enables direct privilege escalation: an attacker can set the setuid bit on any binary, change ownership of sensitive files, or make system configuration world-writable.

This vulnerability is associated with program files `lib/ssh/src/ssh_sftpd.erl` and program routines `ssh_sftpd:do_open/4` and `ssh_sftpd:handle_op/4`.

This issue affects OTP from OTP 17.0 until OTP 28.4.3, 27.3.4.11, and 26.2.5.20 corresponding to `ssh` from 3.01 until 5.5.3, 5.2.11.7, and 5.1.4.15.

Affected

`pkg:otp/ssh`

Module	Source File	Routine
ssh_sftpd	src/ssh_sftpd.erl	ssh_sftpd:do_open/4 ssh_sftpd:handle_op/4

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	`3.01`	• unaffected at `5.5.3` • unaffected at `5.2.11.7` • unaffected at `5.1.4.15`

pkg:github/erlang/otp

Module	Source File	Routine
ssh_sftpd	lib/ssh/src/ssh_sftpd.erl	ssh_sftpd:do_open/4 ssh_sftpd:handle_op/4

Status	Type	Version	Changes / Fixed in
Affected	otp ⓘ	17.0	• unaffected at 28.4.3 • unaffected at 27.3.4.11 • unaffected at 26.2.5.20
Affected	git ⓘ	07b8f441ca	• unaffected at 28c5d5a6c5

Configurations

The SFTP subsystem must be configured with the `root` option in `ssh_sftpd:subsystem_spec/1`. The `root` option is not set by default.

Workarounds

- Do not use the `root` option in `ssh_sftpd:subsystem_spec/1`, and instead rely on OS-level chroot or container isolation to confine SFTP users.
- Ensure the Erlang VM is not running as a privileged OS user. Running the VM as an unprivileged user limits the impact of this vulnerability, since attribute modifications are constrained by that user's OS-level permissions.

References

- https://github.com/erlang/otp/security/advisories/GHSA-28jg-mw9x-hpm5 vendor-advisory related
- https://osv.dev/vulnerability/EEF-CVE-2026-32147 related
- https://github.com/erlang/otp/commit/28c5d5a6c5f873dc701b597276271763e7d1c004 patch

Credits

- **Finder**: John Downey
- **Remediation developer**: Michał Wąsowski
- **Remediation reviewer**: Jakub Witczak

CVE record as JSON: GET /cves/CVE-2026-32147.json
OSV record as JSON: GET /osv/EEF-CVE-2026-32147.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