Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in SFTP chroot

Moderate **Mikaka27** published **GHSA-28jg-mw9x-hpm5** 1 hour ago

Package

OTP

Affected versions	Patched versions
>= 17.0	28.4.3, 27.3.4.11, 26.2.5.20

ssh (OTP)

>= 3.0.1	5.5.2, 5.2.11.7, 5.1.4.15

Description

Impact

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.

This is a path traversal vulnerability (CWE-22) that breaks the SFTP `root` directory confinement. 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 (e.g., `/tmp/x`). An attacker with write access to the
chroot can create the corresponding path inside the chroot (`{root}/tmp/x`) to obtain a handle, then use `SSH_FXP_FSETSTAT` to modify attributes of the real `/tmp/x`.

Note that this vulnerability only allows modification of file *attributes* (permissions, ownership, timestamps) — 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.

Workarounds

For vulnerable versions, the recommended mitigation is to 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.

Additionally, ensure the Erlang VM is not running as a privileged OS user (see terminology for details on the VM user concept).
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.

Affected/Unaffected Versions

A version larger than or equal to one of the listed *patched versions* is **unaffected**; *otherwise*, a version that satisfies an
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 prior to the introduction of the new *OTP version scheme* are never listed since it is not well defined how to compare those versions.

Credits

Thanks to John Downey for finding and responsibly disclosing this vulnerability to the Erlang/OTP project.

Severity

Moderate 5.3 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-32147

Weaknesses

▶ CWE-22

Credits

jtdowney	Reporter
Mikaka27	Remediation developer
u3s	Remediation reviewer