EEF-CVE-2026-32147

See a problem?
Please try reporting it to the source first.

Source	https://cna.erlef.org/osv/EEF-CVE-2026-32147.html
Import Source	https://cna.erlef.org/osv/EEF-CVE-2026-32147.json
JSON Data	https://api.osv.dev/v1/vulns/EEF-CVE-2026-32147
Aliases	CVE-2026-32147 GHSA-28jg-mw9x-hpm5
Published	2026-04-21T12:01:20.350Z
Modified	2026-04-21T12:26:24.033654844Z
Severity	5.3 (Medium) CVSS_V4 - 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 CVSS Calculator
Summary	SFTP chroot bypass via path traversal in SSH_FXP_FSETSTAT
Details	

Summary

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.

Workaround

- 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.

Configuration

The SFTP subsystem must be configured with the root option in ssh*sftpd:subsystem*spec/1. The root option is not set by default.

Database specific


```
{
    "cpe_ids": [
        "cpe:2.3:a:erlang:erlang\\/otp:*:*:*:*:*:*:*:*"
    ],
    "capec_ids": [],
    "cwe_ids": [
        "CWE-22"
    ]
}
```


References

https://github.com/erlang/otp/security/advisories/GHSA-28jg-mw9x-hpm5

https://cna.erlef.org/cves/CVE-2026-32147.html

https://www.erlang.org/doc/system/versions.html#order-of-versions

https://github.com/erlang/otp/commit/28c5d5a6c5f873dc701b597276271763e7d1c004

Credits

John Downey - FINDER

Michał Wąsowski - REMEDIATION_DEVELOPER

Jakub Witczak - REMEDIATION_REVIEWER

Affected packages

Git
github.com/erlang/otp

Affected ranges

Type GIT

Repo https://github.com/erlang/otp

Events Introduced
07b8f441ca711f9812fad9e9115bab3c3aa92f79
Fixed
28c5d5a6c5f873dc701b597276271763e7d1c004

Affected versions

- OTP-17.*
- OTP-18.*
- OTP-19.*
- OTP-20.*
- OTP-21.*
- OTP-22.*
- OTP-23.*
- OTP-24.*
- OTP-25.*
- OTP-26.*
- Other

Database specific

▸ source