Sandbox escape: file write via symlink at FOD `.tmp` copy destination

Critical **xokdvium** published **GHSA-g3g9-5vj6-r3gj** yesterday

Package

Nix (nix)

Affected versions

>=2.18.2,>=2.19.4,>=2.20.5,>=2.21

Patched versions

2.34.5,2.33.4,2.32.7,2.31.4,2.30.4,2.29.3,2.28.6

Description

Impact

A bug in the fix for CVE-2024-27297 allowed for arbitrary overwrites of files writable by the Nix process orchestrating the builds (typically the Nix daemon running as root in multi-user installations) by following symlinks during fixed-output derivation output registration. This affects sandboxed Linux builds - sandboxed macOS builds are unaffected. The location of the temporary output used for the output copy was located inside the build chroot. A symlink, pointing to an arbitrary location in the filesystem, could be created by the derivation builder at that path. During output registration, the Nix process (running in the host mount namespace) would follow that symlink and overwrite the destination with the derivation's output contents.

In multi-user installations, this allows all users able to submit builds to the Nix daemon (`allowed-users` - defaulting to all users) to gain root privileges by modifying sensitive files.

Fix

The issue is fixed in 2.34.5, 2.33.4, 2.32.7, 2.31.4, 2.30.4, 2.29.3, 2.28.6. The temporary output copy is now created in a directory in the store that is inaccessible to other users.

Patches for versions 2.31, 2.32, 2.33 and 2.34 also include additional hardening to prevent communication and file descriptor smuggling between cooperating fixed-output-derivations via abstract Unix sockets. This hardening is effective on kernels ≥ 6.12 with the landlock LSM enabled. On older kernels, it is skipped. This mitigation is ineffective at preventing communication between fixed-output derivations and processes running outside the Nix sandbox.

Workarounds

Do not allow untrusted builds to be submitted to the Nix daemon (via the `allowed-users` setting or by making the `/nix/var/nix/daemon-socket` directory inaccessible to untrusted users).

References

- #10178, `a3163b9` - patch that introduced the vulnerability for versions >=2.21
- Vulnerable backport to 2.18 `4bc5a35`
- Vulnerable backport to 2.19 `7794354`
- Vulnerable backport to 2.20 `244f3ee`

Severity

Critical 9.0 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	None

Learn more about base metrics

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

CVE ID

CVE-2026-39860

Weaknesses

▶ CWE-61

Credits


edef1c Reporter


xokdvium Remediation developer