Security Advisory: Local privilege escalation in Lix and Nix

RaitoBezarius 1 May 4, 2026, 7:09pm

Summary

Nix and Lix daemon implementations are affected by buffer overflows vulnerabilities that allow a local attacker to gain arbitrary code execution as the daemon user (root in multi-user installations).
The vulnerabilities are identified as:

- Nix: GHSA-vh5x-56v6-4368, CVE ID pending attribution by MITRE.
- Lix: CVE ID pending attribution by MITRE.

This is a coordinated disclosure between the Nix and Lix projects.

Guix is *NOT* affected by this vulnerability.

Am I affected?

To exploit this issue, a local attacker needs access to talk to the Nix daemon. All systems that allow connections to their daemons are affected. Only users that are allowed to connect to the daemon (via `allowed-users` and `trusted-users`) can reliably trigger the issue. Substituters can in theory trigger the issue but cannot make enough attempts to mount attacks in practice.

Additionally, this vulnerability requires ASLR weakening techniques to lead to a compromise.

Fixes

The vulnerabilities are fixed in the following versions:

- Nix:
  - Affected versions: ≥ 2.24.4
  - Fixed versions: 2.34.7, 2.33.6, 2.32.8, 2.31.5, 2.30.5, 2.29.4, 2.28.7
  - Nixpkgs PRs:
    - 25.11: [Backport 25.11] nix: bump all versions to latest patch releases by Mic92 · Pull Request #516633 · NixOS/nixpkgs · GitHub
    - unstable:
    - nix: 2.34.6 -> 2.34.7 by Mic92 · Pull Request #516608 · NixOS/nixpkgs · GitHub.
    - nix: bump 2.28.6 -> 2.28.7, 2.30.4 -> 2.30.5, 2.31.4 -> 2.31.5 by Mic92 · Pull Request #516612 · NixOS/nixpkgs · GitHub

Nix security release also includes patches that address an unrelated path traversal vulnerability GHSA-gr92-w2r5-qw5p (CVE ID pending attribution).

- Lix:
  - Affected versions: ≥ 2.93.0
  - Fixed versions: 2.93.4, 2.94.2, 2.95.2
  - Nixpkgs PRs:
    - 25.11: **[25.11] lix_2_9{3,4,5}: 2.9{3,4,5}.{3,1} -> 2.9{3,4,5}.{4,2} by RaitoBezarius · Pull Request #516597 · NixOS/nixpkgs · GitHub**.
    - unstable:
    - **lix_2_9{4,5}: 2.9{4,5}.1 -> 2.9{4,5}.2 by RaitoBezarius · Pull Request #516590 · NixOS/nixpkgs · GitHub** **GitHub - NixOS/nixpkgs: Nix Packages collection & NixOS · GitHub** pull/516606
  - In-depth blog post on the vulnerability: later.

To make exploiting this class of vulnerabilities harder, NixOS has been patched to increase the effectiveness of ASLR **#510943**.

Acknowledgement

- We would like to thank @edef with the help of Sander (@sandydoo) for reporting the issues and working with the development teams to suggest and confirm the fixes.
- Thanks to eldritch horrors (@pennae) and Raito Bezarius (@RaitoBezarius) on the Lix side for the mitigation.
- Thanks to @xokdvium on the Nix side for the mitigation.
- Thanks to @hexa and @tgerbet on the NixOS security team for coordinating this.

35 Likes

---

xokdvium 3 May 4, 2026, 10:13pm

Can’t edit the post, but the Nix update PRs in nixpkgs are:

- 25.11: **[Backport 25.11] nix: bump all versions to latest patch releases by Mic92 · Pull Request #516633 · NixOS/nixpkgs · GitHub**
- unstable **nix: bump 2.28.6 -> 2.28.7, 2.30.4 -> 2.30.5, 2.31.4 -> 2.31.5 by Mic92 · Pull Request #516612 · NixOS/nixpkgs · GitHub** (bumps everything but 2.34, that was done in **nix: 2.34.6 -> 2.34.7 by Mic92 · Pull Request #516608 · NixOS/nixpkgs · GitHub**)

4 Likes