Message-ID: <CAPC5pGQG0JGK0Nh+9UMLzaqT+3SZ-cD1eQdLjsWeLds-YAyWrg@mail.gmail.com>
Date: Mon, 4 May 2026 23:06:14 +0200
From: Thomas GERBET <thomas@...bet.me>
To: oss-security@...ts.openwall.com
Subject: Local privilege escalation in Lix and Nix

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.
- Lix: CVE ID pending attribution.

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

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

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.

References

*
https://discourse.nixos.org/t/security-advisory-local-privilege-escalation-in-lix-and-nix/77407
* Nix issues:
  - https://github.com/NixOS/nix/security/advisories/GHSA-vh5x-56v6-4368
  - https://github.com/NixOS/nix/security/advisories/GHSA-gr92-w2r5-qw5p

```
* Lix in-depth review blog post: not yet published
```