Coroutine stack-to-heap overflow via unbounded recursion in NAR directory parser

High **edolstra** published **GHSA-vh5x-56v6-4368** 7 hours ago

Package

nix (Nix)

Affected versions

>=2.24.4

Patched versions

2.34.7,2.33.6,2.32.8,2.31.5,2.30.5,2.29.4,2.28.7

Description

Impact

Unbounded recursion in the NAR (Nix Archive) parser could lead to a stack-to-heap overflow when the parser is run on a coroutine stack. The stack was allocated without a guard page, which meant that a stack overflow could overwrite memory on the heap and could allow for arbitrary code execution as the Nix daemon (run as root in multi-user installations) if ASLR hardening is bypassed. This vulnerability can be exploited by all users able to connect to the Nix daemon (configurable via `allowed-users` setting - all users by default).

The vulnerability is present since 2.24.4.

Fix

NAR directory recursion depth is now limited to 64 levels and enforced during parsing and serialisation, coroutine stacks are allocated with a guard page. As additional hardening, symlink entries in the NAR are now checked for invalid contents, archive entries and metadata/tag length is now bounded (255 bytes for file names - same as NAME_MAX on Linux and 4096 for symlink target length). The Nix daemon now also limits the number of forked worker crashes to 64 to mitigate attacks that would require bypassing ASLR.

Fixed versions are 2.34.7, 2.33.6, 2.32.8, 2.31.5, 2.30.5, 2.29.4, 2.28.7.

References

- PR introducing the vulnerability #11152.
- Vulnerable backport to 2.24 #11360.

Severity

High 7.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

No known CVE

Weaknesses

- CWE-674
- CWE-787

Credits

 **edef1c** Reporter

 **sandydoo** Finder