Absolute path traversal when unpacking archives to disk

Moderate **edolstra** published **GHSA-gr92-w2r5-qw5p** 7 hours ago

Package

nix (Nix)

Affected versions

>=2.24.7

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

When an archive (e.g. a tarball) contains entries with absolute paths, `nix-prefetch-url --unpack`, `nix store prefetch-file --unpack` commands would write to a location outside the extraction root. This also affects `builtin:unpack-channel` builtin derivation builder, but it's sandboxed the same way as regular derivations builds, so in sandboxed builds it can't be used to achieve an arbitrary file write on the host filesystem.

Other archive unpacking (`builtins.fetchTarball`, `builtins.fetchTree` and tarball-based flake inputs) is not affected, since Nix stores the unpacked tarball in a bare git repository (`.cache/nix/tarball-cache` or `.cache/nix/tarball-cache-v2`).

This primarily affects packagers running `nix-prefetch-url --unpack` on untrusted archives.

The vulnerability is present since 2.24.7.

Fix

The vulnerability is fixed in 2.34.7, 2.33.6, 2.32.8, 2.31.5, 2.30.5, 2.29.4, 2.28.7.

Workarounds

Do not run `nix-prefetch-url --unpack` and `nix store prefetch-file` on untrusted inputs.

Severity

Moderate 4.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

No known CVE

Weaknesses

▶ CWE-36

Credits

 **edef1c** Reporter