



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-39860
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 21:17:00 UTC
Updated	2026-04-08 21:26:13 UTC

Description Nix is a package manager for Linux and other Unix systems. A bug in the fix for CVE-2024-27297 allowed for arbitrary over

Risk And Classification

Primary CVSS: v3.1 9 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-61 | CWE-61 CWE-61: UNIX Symbolic Link (Symlink) Following

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9	CRITICAL	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	DECLARED	9	CRITICAL	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NixOS	Nix	affected >= 2.21, < 2.28.6	Not specified
CNA	NixOS	Nix	affected >= 2.29.0, < 2.29.3	Not specified
CNA	NixOS	Nix	affected >= 2.30.0, < 2.30.4	Not specified
CNA	NixOS	Nix	affected >= 2.31.0, < 2.31.4	Not specified
CNA	NixOS	Nix	affected >= 2.32.0, < 2.32.7	Not specified
CNA	NixOS	Nix	affected >= 2.33.0, < 2.33.4	Not specified
CNA	NixOS	Nix	affected >= 2.34.0, < 2.34.5	Not specified
CNA	NixOS	Nix	affected >= 2.20.5, <= 2.20.9	Not specified
CNA	NixOS	Nix	affected >= 2.19.4, <= 2.19.7	Not specified
CNA	NixOS	Nix	affected >= 2.18.2, <= 2.18.9	Not specified

References

Reference	Source	Link	Tags
github.com/NixOS/nix/pull/10178	security-advisories@github.com	github.com	
github.com/NixOS/nix/commit/4bc5a3510fa3735798f9ed3a2a30a3ea7b32343a	security-advisories@github.com	github.com	
github.com/NixOS/nix/commit/a3163b9eabb952b4aa96e376dea95ebcca97b31a	security-advisories@github.com	github.com	
github.com/NixOS/nix/security/advisories/GHSA-g3g9-5vj6-r3gj	security-advisories@github.com	github.com	
github.com/NixOS/nix/commit/7794354a982449927ee7401cdeb573ddd16c4688	security-advisories@github.com	github.com	
github.com/NixOS/nix/commit/244f3eee0bbc7f11e9b383a15ed7368e2c4becc9	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report