CVE-2026-29645

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-29645
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 20:16:48 UTC
Updated	2026-04-24 19:25:35 UTC
Description	NEMU (OpenXiangShan/NEMU) before v2025.12.r2 contains an improper instruction-validation flaw in its RISC-V Vector (F

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

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

EPSS: 0.000310000 probability, percentile 0.090540000 (date 2026-04-27)

Problem Types: CWE-131 | CWE-1287 | n/a | CWE-131 CWE-131 Incorrect Calculation of Buffer Size | CWE-1287 CWE-1287 Improper Validation of Specified Type of Input

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xiangshan	Nemu	2025.12	r1	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
github.com/OpenXiangShan/NEMU/commit/481de637d5fc5838356caee80a79e56a337...	cve@mitre.org	github.com	Patch
github.com/OpenXiangShan/NEMU/pull/958	cve@mitre.org	github.com	Issue Tracking
docs.riscv.org/reference/isa/unpriv/v-st-ext.html	cve@mitre.org	docs.riscv.org	Product
github.com/OpenXiangShan/NEMU/issues/952	cve@mitre.org	github.com	Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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