



# CVE-2026-29645

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

## Summary

<b>CVE</b>	CVE-2026-29645
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-20 20:16:48 UTC
<b>Updated</b>	2026-04-24 19:25:35 UTC
<b>Description</b>	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)