LoongArch: KVM: Handle the case that EIOINTC's coremap is empty

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

Summary

CVE	CVE-2026-31569
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:31 UTC
Updated	2026-04-27 20:33:04 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Handle the case that EIOINTC's corema

Risk And Classification

Primary CVSS: v3.1 7.3 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000170000 probability, percentile 0.040590000 (date 2026-04-27)

Problem Types: CWE-125

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:H
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

ntegrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 3956a52bc05bd811082a3c9d2b423ee957e6fefc 126053d0a685bf1f2e98db8966386f38b2336338 git
CNA	Linux	Linux	affected 3956a52bc05bd811082a3c9d2b423ee957e6fefc 2a0cbcd28ecf6e0b88fa498bebb94bd1be61a7c3 git
CNA	Linux	Linux	affected 3956a52bc05bd811082a3c9d2b423ee957e6fefc b97bd69eb0f67b5f961b304d28e9ba45e202d841 git
CNA	Linux	Linux	affected 6.13
CNA	Linux	Linux	unaffected 6.13 semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/126053d0a685bf1f2e98db8966386f38b2336338	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2a0cbcd28ecf6e0b88fa498bebb94bd1be61a7c3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b97bd69eb0f67b5f961b304d28e9ba45e202d841	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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