



LoongArch: KVM: Fix base address calculation in `kvm_eiointc_regs_access()`

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-31564 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-24 15:16:30 UTC |
| Updated | 2026-04-27 20:31:10 UTC |
| Description | In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Fix base address calculation in <code>kvm_eiointc_regs_access()</code> |

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000180000 probability, percentile 0.049720000 (date 2026-04-27)

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/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 |
| Operating System | Linux | Linux Kernel | 6.19 | - | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc1 | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc2 | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc3 | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc4 | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc5 | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc6 | All | All |
| Operating System | Linux | Linux Kernel | 7.0 | rc7 | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------------------|-----------------------|--|
| CNA | Linux | Linux | affected d3e43a1f34acbb9a814337fc5624765538e5a274 c4f0a9481cf0dd7c71a07484bc98f2570fdb3a82 git |
| CNA | Linux | Linux | affected d3e43a1f34acbb9a814337fc5624765538e5a274 6bcfb7f46d667b04bd1a1169ccedf5fb699c60df git |
| CNA | Linux | Linux | affected 6.19 |
| CNA | Linux | Linux | unaffected 6.19 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/6bcfb7f46d667b04bd1a1169ccedf5fb699c60df | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| git.kernel.org/stable/c/c4f0a9481cf0dd7c71a07484bc98f2570fdb3a82 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch |
| 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.

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