



Out-of-bounds Write in Firecracker virtio-pci Transport

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-5747 |
| State | PUBLISHED |
| Assigner | AMZN |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-08 00:16:05 UTC |
| Updated | 2026-04-20 16:16:49 UTC |
| Description | An out-of-bounds write issue in the virtio PCI transport in Firecracker 1.13.0 through 1.14.3 and 1.15.0 on x86_64 and aarch64. |

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from ff89ba41-3aa1-4d27-914a-91399e9639e5

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000180000 probability, percentile 0.047520000 (date 2026-04-21)

Problem Types: CWE-369 | CWE-787 | CWE-787 CWE-787 Out-of-bounds write | CWE-369 CWE-369 Divide by zero

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 4.0 | ff89ba41-3aa1-4d27-914a-91399e9639e5 | Secondary | 8.7 | HIGH | CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0 | CNA | CVSS | 8.7 | HIGH | CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 3.1 | ff89ba41-3aa1-4d27-914a-91399e9639e5 | Secondary | 7.5 | HIGH | CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 7.5 | HIGH | CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H |

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------|-------------|-------------------------------|---------------|
| CNA | AWS | Firecracker | affected 1.13.0 1.14.3 custom | Not specified |
| CNA | AWS | Firecracker | affected 1.15.0 | Not specified |
| CNA | AWS | Firecracker | unaffected 1.14.4 | Not specified |

References

| Reference | Source | Link |
|---|--------------------------------------|---|
| github.com/firecracker-microvm/firecracker/security/advisories/GHSA-776c... | ff89ba41-3aa1-4d27-914a-91399e9639e5 | github.com |
| github.com/firecracker-microvm/firecracker/releases/tag/v1.14.4 | ff89ba41-3aa1-4d27-914a-91399e9639e5 | github.com |
| aws.amazon.com/security/security-bulletins/2026-015-aws | ff89ba41-3aa1-4d27-914a-91399e9639e5 | aws.amazon.com |
| github.com/firecracker-microvm/firecracker/releases/tag/v1.15.1 | ff89ba41-3aa1-4d27-914a-91399e9639e5 | github.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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