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

High **JackThomson2** published **GHSA-776c-mpj7-jm3r** 13 minutes ago

Package

Firecracker

Affected versions

>=1.13.0, <= 1.14.3, 1.15.0

Patched versions

1.14.4, 1.15.1

Description

Summary

Firecracker is an open source virtualization technology that is purpose-built for creating and managing secure, multi-tenant container and function-based services. An issue exists where, under certain circumstances, a root-privileged guest can modify virtio queue configuration registers after device activation in the virtio PCI transport, bypassing bounds validation performed during initialization.

Impact

After device activation, a root-privileged guest can modify the queue_size register, which was already validated during initialization. This can cause

- A process panic (denial of service) via divide-by-zero
- Out-of-bounds writes up to 524,284 bytes beyond the virtio queues

Simply modifying queue_size only results in OOB access beyond the virtio queues but within guest memory on a standard Linux kernel. To achieve OOB access beyond guest memory into the Firecracker process's host memory, additional preconditions must be satisfied that require a higher level of control over the guest environment, such as the use of a custom guest kernel or specific snapshot configurations.

Impacted versions: >= 1.13.0 AND <= 1.14.3 AND 1.15.0

Patches

This issue has been addressed in Firecracker versions 1.14.4 and 1.15.1. We recommend upgrading to the latest version and ensuring any forked or derivative code is patched to incorporate the new fixes.

Workarounds

The virtio PCI transport is opt-in via the `--enable-pci` command-line flag when starting Firecracker. The legacy MMIO transport is the default and is not affected by this issue. Users who have enabled PCI transport can revert to MMIO by removing the `--enable-pci` flag from their Firecracker invocation. Note that switching from PCI to MMIO transport may result in reduced I/O throughput and increased latency.

References

If you have any questions or comments about this advisory, we ask that you contact AWS Security via our vulnerability reporting page or directly via email to aws-security@amazon.com. Please do not create a public GitHub issue.

Acknowledgement

We would like to thank Xinyang Ge (**@aegiryy**) and Claude (**@claude**) for reporting this concern to the AWS Vulnerability Disclosure Program

Severity

High 8.7 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Local
Attack Complexity	High
Attack Requirements	Present
Privileges Required	High
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-5747

Weaknesses

- CWE-369
- CWE-787