



CVE-2023-41051

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

Summary

CVE	CVE-2023-41051
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-01 19:15:00 UTC
Updated	2023-09-28 03:15:00 UTC
Description	In a typical Virtual Machine Monitor (VMM) there are several components, such as boot loader, virtual device drivers, virtio I/O devices, and so on. The boot loader is responsible for loading the operating system kernel and initializing the hardware. The virtual device drivers are responsible for emulating the hardware devices. The virtio I/O devices are responsible for providing a high-performance interface between the guest operating system and the host operating system. The boot loader, virtual device drivers, and virtio I/O devices are all critical components of the VMM. If any of these components are compromised, the VMM may be vulnerable to attack. This CVE describes a vulnerability in the boot loader of the VMM. The vulnerability allows an attacker to bypass the boot loader's security checks and load a malicious operating system kernel. This could lead to a complete compromise of the VMM and the guest operating system.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vm-memory Project	Vm-memory	All	All	All	All

References

Reference
[SECURITY] Fedora 37 Update: firecracker-1.4.1-2.fc37 - package-announce - Fedora Mailing-Lists
fix: Validate return value of get_slice in VolatileMemory · rust-vmm/vm-memory@aff1dd4 · GitHub
crates.io/crates/vm-memory/0.12.2
[SECURITY] Fedora 38 Update: libkrun-1.5.0-6.fc38 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 39 Update: virtiofsd-1.7.0-4.fc39 - package-announce - Fedora Mailing-Lists
Default functions in VolatileMemory trait lack bounds checks, potentially leading to out-of-bounds memory accesses · Advisory · rust-vmm/vm-memory
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284548](#) Fedora Security Update for firecracker (FEDORA-2023-1db67725f2)

[284553](#) Fedora Security Update for firecracker (FEDORA-2023-c19aaa2283)

[285252](#) Fedora Security Update for firecracker (FEDORA-2023-8e6ae98f81)

© [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](#)