



CVE-2023-42467

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

Summary

CVE	CVE-2023-42467
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-11 04:15:00 UTC
Updated	2023-11-04 06:15:00 UTC
Description	QEMU through 8.0.0 could trigger a division by zero in scsi_disk_reset in hw/scsi/scsi-disk.c because scsi_disk_emulate_m

Risk And Classification

Problem Types: CWE-369

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source
FPE division by zero in scsi_disk_reset() (#1813) · Issues · QEMU / QEMU · GitLab	MISC
hw/scsi/scsi-disk: Disallow block sizes smaller than 512 [CVE-2023-42467] (7cfcc79b) · Commits · QEMU / QEMU · GitLab	MISC
hw/scsi/scsi-disk: Disallow block sizes smaller than BDRV_SECTOR_SIZE (3f911044) · Commits · Thomas Huth / QEMU · GitLab	MISC
CVE-2023-42467 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIR
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161478 Oracle Enterprise Linux Security Update for virt:kvm_utils3 (ELSA-2024-12276)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)