



CVE-2023-3180

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

Summary

CVE	CVE-2023-3180
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-03 15:15:00 UTC
Updated	2023-11-07 14:50:00 UTC
Description	A flaw was found in the QEMU virtual crypto device while handling data encryption/decryption requests in virtio_crypto_han

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	-	All	All	All
Application	Qemu	Qemu	8.1.0	rc0	All	All
Application	Qemu	Qemu	8.1.0	rc1	All	All
Application	Qemu	Qemu	8.1.0	rc2	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3604-1] qemu security update	MISC	lists.
CVE-2023-3180 QEMU Vulnerability in NetApp Products NetApp Product Security	MISC	secu
cve-details	MISC	acce
2222424 – (CVE-2023-3180) CVE-2023-3180 QEMU: virtio-crypto: heap buffer overflow in virtio_crypto_sym_op_helper()	MISC	bugz
[SECURITY] Fedora 38 Update: qemu-7.2.5-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160940](#) Oracle Enterprise Linux Security Update for qemu (ELSA-2023-12834)

[160941](#) Oracle Enterprise Linux Security Update for qemu (ELSA-2023-12835)

[160960](#) Oracle Enterprise Linux Security Update for kvm_utils3 (ELSA-2023-12855)

[161346](#) Oracle Enterprise Linux Security Update for virt:kvm_utils1 (ELSA-2024-12152)

[355861](#) Amazon Linux Security Advisory for qemu : ALAS2-2023-2207

[6000126](#) Debian Security Update for qemu (DLA 3604-1)

[673490](#) EulerOS Security Update for qemu (EulerOS-SA-2023-2887)

[673611](#) EulerOS Security Update for qemu-micro (EulerOS-SA-2023-3193)

[673919](#) EulerOS Security Update for qemu (EulerOS-SA-2023-2906)

[674008](#) EulerOS Security Update for qemu-micro (EulerOS-SA-2023-3228)

[754898](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3721-1)

[754937](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3800-1)

[755084](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:4056-1)

[755817](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2024:0589-1)

© [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](#)