



CVE-2022-0216

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

Summary

CVE	CVE-2022-0216
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-26 18:15:00 UTC
Updated	2023-02-12 22:15:00 UTC
Description	A use-after-free vulnerability was found in the LSI53C895A SCSI Host Bus Adapter emulation of QEMU. The flaw occurs w

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Li
scsi/lsi53c895a: really fix use-after-free in lsi_do_msgout (CVE-2022-0216) (4367a20c) · Commits · QEMU / QEMU · GitLab	MISC	gi
[SECURITY] Fedora 37 Update: qemu-7.0.0-10.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lis
2036953 – (CVE-2022-0216) CVE-2022-0216 QEMU: use-after-free in lsi_do_msgout function in hw/scsi/lsi53c895a.c	MISC	bu
[SECURITY] Fedora 37 Update: qemu-7.0.0-10.fc37 - package-announce - Fedora Mailing-Lists	MISC	lis
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	ac
LSI SCSI Use After Free (CVE-2022-0216) (#972) · Issues · QEMU / QEMU · GitLab	MISC	gi
(CVE-2022-0216) QEMU LSI SCSI Use After Free STAR Labs	MISC	st
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160134	Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2022-9869)
160141	Oracle Enterprise Linux Security Update for kvm_utils2 (ELSA-2022-9862)
160201	Oracle Enterprise Linux Security Update for qemu (ELSA-2022-9978)
160203	Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9986)
181630	Debian Security Update for qemu (DLA 3362-1)
182012	Debian Security Update for qemu (CVE-2022-0216)
199069	Ubuntu Security Notification for QEMU Vulnerabilities (USN-5772-1)
283051	Fedora Security Update for qemu (FEDORA-2022-baf3c3b781)
283467	Fedora Security Update for qemu (FEDORA-2022-4387579e67)
752675	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3594-1)
752685	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3660-1)
752725	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3768-1)
752746	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3795-1)
753802	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)
753824	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0840-1)
903756	Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (10781)

© [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](#)