CVE-2021-3392

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3392
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-23 20:15:00 UTC
Updated	2022-09-30 19:48:00 UTC
Description	A use-after-free flaw was found in the MegaRAID emulator of QEMU. This issue occurs while processing SCSI I/O requests

Risk And Classification

Problem Types: CWE-416

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
1924042 – (CVE-2021-3392) CVE-2021-3392 QEMU: scsi: mptsas: use-after-free while processing io requests	MISC	bugzilla.redhat
Bug #1914236 “QEMU: scsi: use-after-free in mptsas_process_scsi_...” : Bugs : QEMU	MISC	bugs.launchpa
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.org
[SECURITY] [DLA 2623-1] qemu security update	MLIST	lists.debian.org
March 2021 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159368 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9425)

159465 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9425)

159566 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2021-9568)

178540 Debian Security Update for qemu (DLA 2623-1)

179672 Debian Security Update for qemu (CVE-2021-3392)

180995 Debian Security Update for qemu (DLA 3099-1)

198432 Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)

355320 Amazon Linux Security Advisory for qemu : ALAS2-2023-2061

502354 Alpine Linux Security Update for qemu

671198 EulerOS Security Update for qemu (EulerOS-SA-2022-1034)

671203 EulerOS Security Update for qemu (EulerOS-SA-2022-1014)

900218 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

903075 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (4020)

© 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 registred 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