



CVE-2020-29443

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

Summary

CVE	CVE-2020-29443
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:15:00 UTC
Updated	2022-09-30 19:17:00 UTC
Description	ide_atapi_cmd_reply_end in hw/ide/atapi.c in QEMU 5.1.0 allows out-of-bounds read access because a buffer index is not

Risk And Classification

Problem Types: CWE-125

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	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	5.1.0	-	All	All
Application	Qemu	Qemu	5.1.0	-	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2560-1] qemu security update	MLIST	lists.debian.org	Mailir
CVE-2020-29443 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Third
oss-security - CVE-2020-29443 QEMU: ide: atapi: OOB access while processing read commands	MISC	www.openwall.com	Mailir
[PATCH] ide:atapi: check io_buffer_index in ide_atapi_cmd_reply_end	MISC	lists.nongnu.org	Mailir
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159252	Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2021-2322)
159456	Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-1762)
174920	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1243-1)
174921	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
174922	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
174923	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
174924	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
174926	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
180995	Debian Security Update for qemu (DLA 3099-1)
198432	Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)
239306	Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:1762)
239401	Red Hat Update for qemu-kvm (RHSA-2021:2322)
257086	CentOS Security Update for qemu-kvm (CESA-2021:2322)
352383	Amazon Linux Security Advisory for qemu: ALAS2-2021-1671
377413	Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
377549	Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2021:0035)
502353	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)
750251	OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)
940118	AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:1762)
960265	Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:1762)

© [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](#).

