



CVE-2020-13659

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

Summary

CVE	CVE-2020-13659
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-02 13:15:00 UTC
Updated	2022-11-16 03:37:00 UTC
Description	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Qemu	Qemu	4.2.0	All	All	All
Application	Qemu	Qemu	4.2.0	All	All	All

References

Reference	Source
Re: [PATCH v4] exec: set map length to zero when returning NULL	MISC
[SECURITY] [DLA 2288-1] qemu security update	MLIST
Debian -- Security Information -- DSA-4728-1 qemu	DEBIAN
oss-security - CVE-2020-13659 QEMU: exec: address_space_map returns NULL without setting length to zero may lead to DoS	CONFIRM
QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security	GENTOO
June 2020 QEMU Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM
USN 4467-1: QEMU vulnerabilities Ubuntu security notices Ubuntu	UBUNTU

OSIN-4467-1: QEMU vulnerabilities Ubuntu Security Notices Ubuntu	UBUNTU
[security-announce] openSUSE-SU-2020:1108-1: important: Security update	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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)
502351 Alpine Linux Security Update for qemu
900050 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
902799 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1961)

© 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