



CVE-2020-13754

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

Summary

CVE	CVE-2020-13754
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-02 14:15:00 UTC
Updated	2020-12-14 20:31:00 UTC
Description	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x m

Risk And Classification

Problem Types: CWE-119

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	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	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
oss-security - CVE-2020-13754 QEMU: msix: OOB access during mmio operations may lead to DoS	CONFIRM	www.openwall.com
[SECURITY] [DLA 2288-1] qemu security update	MLIST	lists.debian.org
oss-security - Re: CVE-2020-13754 QEMU: msix: OOB access during mmio operations may lead to DoS	MLIST	www.openwall.com

Debian -- Security Information -- DSA-4728-1 qemu	DEBIAN	www.debian.org
QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security	GENTOO	security.gentoo.org
[PATCH] msix: add valid.accepts methods to check address	MISC	lists.gnu.org
June 2020 QEMU Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
USN-4467-1: QEMU vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
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

- [159343](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-3061)
- [239539](#) Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:3061)
- [377346](#) Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2021:0058)
- [502351](#) 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)
- [750124](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1894-1)
- [750129](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1895-1)
- [750152](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1947-1)
- [753802](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)
- [754898](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:3721-1)
- [900187](#) CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
- [903673](#) Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1955)
- [940064](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:3061)
- [960072](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:3061)

© [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