CVE-2020-13765

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13765
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 16:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	rom_copy() in hw/core/loader.c in QEMU 4.0 and 4.1.0 does not validate the relationship between two addresses, which all

Risk And Classification

Problem Types: CWE-787

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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	4.0.0	All	All	All
Application	Qemu	Qemu	4.1.0	All	All	All
Application	Qemu	Qemu	4.1.0	All	All	All

References

Reference	Source	Link
git.qemu.org Git - qemu.git/commit		git.qem
hw/core/loader: Fix possible crash in rom_copy() · qemu/qemu@4f1c6cb · GitHub	MISC	github.
[SECURITY] [DLA 2262-1] qemu security update	MLIST	lists.de
[SECURITY] [DLA 2288-1] qemu security update	MLIST	lists.de
CVE-2020-13765 QEMU Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	securit
USN-4467-1: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ub

git.qemu.org Git - qemu.git/commit	MISC	git.qem
oss-security - CVE-2020-13765 QEMU: loader: OOB access while loading registered ROM may lead to code execution	CONFIRM	www.o
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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)
- 352242 Amazon Linux Security Advisory for qemu-kvm: ALAS-2021-1488
- 352251 Amazon Linux Security Advisory for qemu: ALAS2-2021-1617
- 377426 Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2021:0008)
- 502350 Alpine Linux Security Update for qemu