CVE-2020-1711

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1711
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-11 20:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	13.0	All	All	All

References

Reference	Source
[PATCH] iscsi: Cap block count from GET LBA STATUS (CVE-2020-1711)	MISC
Red Hat Customer Portal	REDHA
QEMU: Multiple vulnerabilities (GLSA 202005-02) — Gentoo security	GENTO
USN-4283-1: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU
oss-security - CVE-2020-1711 QEMU: block: iscsi: OOB heap access via an unexpected response of iSCSI Server	MISC
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
1794290 – (CVE-2020-1711) CVE-2020-1711 QEMU: block: iscsi: OOB heap access via an unexpected response of iSCSI Server	CONFIR
[SECURITY] [DLA 2144-1] qemu security update	MLIST
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHA
[SECURITY] [DLA 2373-1] qemu security update	MLIST
[security-announce] openSUSE-SU-2020:0468-1: important: Security update	SUSE
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
- 900050 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
- 903618 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1959)
- 940144 AlmaLinux Security Update for virt:rhel (ALSA-2020:1358)
- 960718 Rocky Linux Security Update for virt:rhel (RLSA-2020:1358)