CVE-2017-16845

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-16845
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-17 20:29:00 UTC
Updated	2020-09-10 17:42:00 UTC
Description	hw/input/ps2.c in Qemu does not validate 'rptr' and 'count' values during guest migration, leading to out-of-bounds access.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
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	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	Tags
USN-3649-1: QEMU vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisory
USN-3575-1: QEMU vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisory

USN-3573-1: QEMU vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisory
[SECURITY] [DLA 1497-1] qemu security update	MLIST	lists.debian.org	Mailing List, Third Par
Debian -- Security Information -- DSA-4213-1 qemu	DEBIAN	www.debian.org	Third Party Advisory
Re: [Qemu-devel] [PATCH v2] ps2: check PS2Queue indices in post_load rou	MLIST	lists.gnu.org	Mailing List, Patch, Th
QEMU 'hw/input/ps2.c' Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party Advisory,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**