CVE-2018-18954

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

Summary

CVE	CVE-2018-18954
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-15 20:29:00 UTC
Updated	2019-05-31 14:29:00 UTC
Description	The pnv_lpc_do_eccb function in hw/ppc/pnv_lpc.c in Qemu before 3.1 allows out-of-bounds write or read access to Power

Risk And Classification

Problem Types: CWE-125 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link
QEMU 'hw/ppc/pnv_lpc.c' Out of Bounds Denial of Service Vulnerability	BID	www.securityfocus.com
[security-announce] openSUSE-SU-2019:1074-1: important: Security update	SUSE	lists.opensuse.org
Re: [Qemu-devel] [PATCH v2] ppc/pnv: check size before data buffer acces	MLIST	lists.gnu.org
USN-3826-1: QEMU vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
oss-security - CVE-2018-18954 QEMU: ppc64: Out-of-bounds r/w stack access in pnv_lpc_do_eccb	MLIST	www.openwall.com
Debian -- Security Information -- DSA-4454-1 qemu	DEBIAN	www.debian.org

Bugtraq: [SECURITY] [DSA 4454-1] qemu security update	BUGTRAQ	seclists.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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