CVE-2019-8934

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

Summary

CVE	CVE-2019-8934
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2022-04-05 20:14:00 UTC
Description	hw/ppc/spapr.c in QEMU through 3.1.0 allows Information Exposure because the hypervisor shares the /proc/device-tree/sy

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.0	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

References

Reference	Source	Link	Tags
oss-security - CVE-2019-8934 QEMU: ppc64: sPAPR emulator leaks the host hardware identity	MISC	www.openwall.com	Maili
QEMU CVE-2019-8934 Local Information Disclosure Vulnerability	MISC	www.securityfocus.com	Third
[security-announce] openSUSE-SU-2019:1405-1: important: Security update	SUSE	lists.opensuse.org	
Re: [Qemu-devel] [PATCH v4] ppc: add host-serial and host-model machine	MISC	lists.gnu.org	Expl
March 2019 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third
[security-announce] openSUSE-SU-2019:1274-1: important: Security update	SUSE	lists.opensuse.org	Maili
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

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**