CVE-2014-3471

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

Summary

CVE	CVE-2014-3471
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-12 17:29:00 UTC
Updated	2018-01-31 14:51:00 UTC
Description	Use-after-free vulnerability in hw/pci/pcie.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	2.1.2	r1	All	All
Application	Qemu	Qemu	2.1.2	r1	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	Tags
[Qemu-devel] [PATCH v2 3/3] hw/pcie: better hotplug/hotunplug support	MLIST	lists.gnu.org	Patch, Third Party
Gentoo Linux Documentation -- QEMU: Multiple Vulnerabilities	GENTOO	security.gentoo.org	Third Party Adviso
oss-security - CVE-2014-3471 Qemu: hw: pci: use after free triggered via guest	MLIST	www.openwall.com	Mailing List, Patch
Bug 1112271 – CVE-2014-3471 Qemu: hw: pci: use after free triggered via guest	CONFIRM	bugzilla.redhat.com	Issue Tracking, Pa
QEMU CVE-2014-3471 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Adviso
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