CVE-2014-3640

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

Summary

CVE	CVE-2014-3640
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-07 19:55:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The sosendto function in slirp/udp.c in QEMU before 2.1.2 allows local users to cause a denial of service (NULL pointer der

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-476 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:L/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All

Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Qemu	Qemu	2.0.0	-	All	All
Application	Qemu	Qemu	2.0.0	rc0	All	All
Application	Qemu	Qemu	2.0.0	rc1	All	All
Application	Qemu	Qemu	2.0.0	rc2	All	All
Application	Qemu	Qemu	2.0.0	rc3	All	All
Application	Qemu	Qemu	2.0.2	All	All	All
Application	Qemu	Qemu	2.1.0	All	All	All
Application	Qemu	Qemu	2.1.0	rc0	All	All
Application	Qemu	Qemu	2.1.0	rc1	All	All
Application	Qemu	Qemu	2.1.0	rc2	All	All
Application	Qemu	Qemu	2.1.0	rc3	All	All
Application	Qemu	Qemu	2.1.0	rc5	All	All
Application	Qemu	Qemu	2.1.1	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Re: [Qemu-devel] [PATCH v2] slirp: udp: fix NULL pointer dereference bec	af854a3a-2127-422b-91ae-364da2661108	lists.nongnu.org
[Qemu-devel] [PATCH v2] slirp: udp: fix NULL pointer dereference because	af854a3a-2127-422b-91ae-364da2661108	lists.nongnu.org
Bug 1144818 – CVE-2014-3640 qemu: slirp: NULL pointer deref in sosendto()	af854a3a-2127-422b-91ae-364da2661108	bugzilla.redhat.(
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat.com
USN-2409-1: QEMU vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubuntu.co
Debian -- Security Information -- DSA-3045-1 qemu	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
Re: [Qemu-devel] [Qemu-stable] [PATCH v2] slirp: udp: fix NULL pointer d	af854a3a-2127-422b-91ae-364da2661108	lists.nongnu.org
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	rhn.redhat.com
Debian -- Security Information -- DSA-3044-1 qemu-kvm	af854a3a-2127-422b-91ae-364da2661108	www.debian.org

Debian -- Security Information -- DSA-3044-1 qemu-kvm	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
Red Hat Customer Portal	MITRE	access.redhat.c
Red Hat Customer Portal	MITRE	access.redhat.c
access.redhat.com | CVE-2014-3640	MITRE	access.redhat.c
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.