CVE-2015-5745

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

Summary

CVE	CVE-2015-5745
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-23 20:15:00 UTC
Updated	2022-02-20 06:45:00 UTC
Description	Buffer overflow in the send_control_msg function in hw/char/virtio-serial-bus.c in QEMU before 2.4.0 allows guest users to c

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arista	Eos	4.12	All	All	All
Operating System	Arista	Eos	4.13	All	All	All
Operating System	Arista	Eos	4.14	All	All	All
Operating System	Arista	Eos	4.15	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	Tags
Arista - Security Advisory 0013	MISC	www.arista.com	
oss-security - CVE request: Qemu: buffer overflow in virtio-serial	MISC	www.openwall.com	Mailing List, Third Party Advisory

[SECURITY] Fedora 21 Update: xen-4.4.3-4.fc21	MISC	lists.fedoraproject.org	Mailing List, Third Party Advisory
virtio-serial: fix ANY_LAYOUT · qemu/qemu@7882080 · GitHub	MISC	github.com	Patch, Third Party Advisory
[SECURITY] Fedora 22 Update: xen-4.5.1-9.fc22	MISC	lists.fedoraproject.org	Mailing List, Third Party Advisory
[SECURITY] Fedora 23 Update: xen-4.5.1-9.fc23	MISC	lists.fedoraproject.org	Mailing List, Third Party Advisory
oss-security - Re: CVE request: Qemu: buffer overflow in virtio-serial	MISC	www.openwall.com	Exploit, Mailing List, Third Party A
[Qemu-devel] [PULL 02/10] virtio-serial: fix ANY_LAYOUT	MISC	lists.gnu.org	Mailing List, Patch, Third Party A
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**