CVE-2015-5239

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

Summary

CVE	CVE-2015-5239
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-23 20:15:00 UTC
Updated	2022-06-05 02:32:00 UTC
Description	Integer overflow in the VNC display driver in QEMU before 2.1.0 allows attachers to cause a denial of service (process cras

Risk And Classification

Problem Types: CWE-835

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	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	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	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

Application	Suse	Linux Enterprise Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All

References

Reference	Source	Link	Tags
oss-security - CVE-2015-5239 Qemu: vnc infinite loop issue	MISC	www.openwall.com	Mailing List, Patch, Third
[security-announce] SUSE-SU-2015:1894-1: important: Security update for	MISC	lists.opensuse.org	Mailing List, Third Party
ui/vnc: limit client_cut_text msg payload size · qemu/qemu@f9a70e7 · GitHub	CONFIRM	github.com	Patch, Third Party Advis
[security-announce] SUSE-SU-2015:1908-1: important: Security update for	MISC	lists.opensuse.org	Mailing List, Third Party
[SECURITY] Fedora 21 Update: xen-4.4.3-4.fc21	MISC	lists.fedoraproject.org	Mailing List, Third Party
Arista - Security Advisory 0014	MISC	www.arista.com	
[SECURITY] Fedora 22 Update: xen-4.5.1-9.fc22	MISC	lists.fedoraproject.org	Mailing List, Third Party
[security-announce] SUSE-SU-2015:1853-1: important: Security update for	MISC	lists.opensuse.org	Mailing List, Third Party
[SECURITY] Fedora 23 Update: xen-4.5.1-9.fc23	MISC	lists.fedoraproject.org	Mailing List, Third Party
USN-2745-1: QEMU vulnerabilities | Ubuntu	MISC	www.ubuntu.com	Third Party Advisory

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