CVE-2015-5225

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

Summary

CVE	CVE-2015-5225
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-06 21:59:00 UTC
Updated	2023-02-13 00:52:00 UTC
Description	Buffer overflow in the vnc_refresh_server_surface function in the VNC display driver in QEMU before 2.4.0.1 allows guest u

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All

References

Reference	Source
access.redhat.com | CVE-2015-5225	MISC

Red Hat Customer Portal	MISC
QEMU CVE-2015-5225 Heap Based Buffer Overflow Vulnerability	BID
Debian -- Security Information -- DSA-3348-1 qemu	DEBIAN
QEMU VNC Heap Overflow Lets Local Guest System Users Deny Service or Gain Privileges on the Host System - SecurityTracker	SECTR
[SECURITY] Fedora 23 Update: qemu-2.4.0-2.fc23	FEDOR
Red Hat Customer Portal	REDHA
[Qemu-devel] [PATCH] vnc: fix memory corruption (CVE-2015-5225)	MLIST
Bug 1255896 – CVE-2015-5225 Qemu: ui: vnc: heap memory corruption in vnc_refresh_server_surface	MISC
Red Hat Customer Portal	REDHA
[SECURITY] Fedora 21 Update: qemu-2.1.3-11.fc21	FEDOR
Red Hat Customer Portal	MISC
[Qemu-devel] [ANNOUNCE] QEMU 2.4.0.1 CVE update released	MLIST
oss-security - CVE-2015-5225 Qemu: ui: vnc: heap memory corruption issue	MLIST
[SECURITY] Fedora 22 Update: qemu-2.3.1-3.fc22	FEDOR
QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security	GENTC
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.