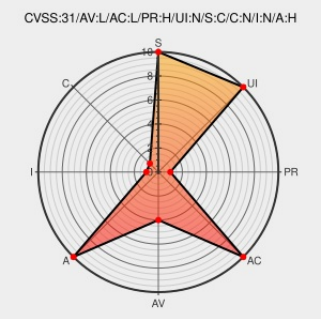
CVE-2016-7422

Published on: 12/09/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:25:00 PM UTC

CVE-2016-7422

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Leap from Opensuse contain the following vulnerability:

The virtqueue_map_desc function in hw/virtio/virtio.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via a large I/O descriptor buffer length value.

CVE-2016-7422 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[Qemu-devel] [PATCH] virtio: add check for descriptor's mapped address	Patch, Third Party Advisory, lists.gnu.org, text/x-diff	MLIST [qemu-devel] 20160915 [PATCH] virtio: add check for descriptor's mapped address

QEMU CVE-2016-7422 Null Pointer Dereference Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 92996
oss-security - CVE request Qemu: virtio: null pointer dereference in virtqueu_map_desc	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160916 CVE request Qemu: virtio: null pointer dereference in virtqueu_map_desc
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:2408
git.qemu.org Git - qemu.git/commit	Patch Vendor Advisory web.archive.org text/xml Inactive Link Not Archived	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=973e7170dddefb491a48df5cba33b2ae151013a0
oss-security - Re: CVE request Qemu: virtio: null pointer dereference in virtqueu_map_desc	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20160916 Re: CVE request Qemu: virtio: null pointer dereference in virtqueu_map_desc
Bug 1376755 – CVE-2016-7422 Qemu: virtio: null pointer dereference in virtqueu_map_desc	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1376755
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:2392
openSUSE-SU-2016:3237-1: moderate: Security update for qemu	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:3237
CVE-2016-7422 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2016-7422
QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201609-01

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All

Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	8.0	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

cpe:2.3:o:opensuse:leap:42.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:10:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:8:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:9:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:10:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization:4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→