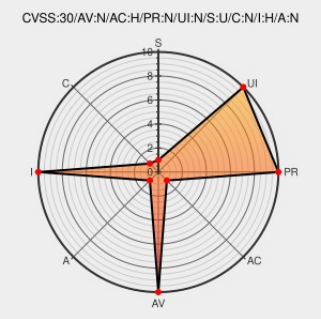
CVE-2011-4600

Published on: 04/14/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:23:00 AM UTC

CVE-2011-4600

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The networkReloadIptablesRules function in network/bridge_driver.c in libvirt before 0.9.9 does not properly handle firewall rules on bridge networks when libvirtd is restarted, which might allow remote attackers to bypass intended access restrictions via a (1) DNS or (2) DHCP query.

CVE-2011-4600 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Bug Access Denied	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=760442
USN-2867-1: libvirt	www.ubuntu.com	UBUNTU USN-2867-1

USN 2007-1: libvirt vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2007-1
libvirt.org Git - libvirt.git/commitdiff	web.archive.org text/xml Inactive Link Not Archived	MISC libvirt.org/git/?p=libvirt.git%3Ba=commitdiff%3Bh=ae1232b298323dd7bef909426e2ebafa6bca9157
libvirt: Releases (2012)	Vendor Advisory web.archive.org text/xml Inactive Link Not Archived	CONFIRM libvirt.org/news-2012.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	15.10	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	15.10	All	All	All
Application	Redhat	Libvirt	0.9.8	All	All	All
Application	Redhat	Libvirt	0.9.8	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:0.9.8:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:0.9.8:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→