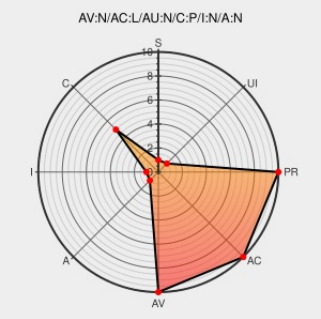
CVE-2014-7823

Published on: 11/13/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:09 AM UTC

CVE-2014-7823

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



Certain versions of Libvirt from Redhat contain the following vulnerability:

The virDomainGetXMLDesc API in Libvirt before 1.2.11 allows remote read-only users to obtain the VNC password by using the VIR_DOMAIN_XML_MIGRATABLE flag, which triggers the use of the VIR_DOMAIN_XML_SECURE flag.

CVE-2014-7823 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Security Advisory SA62303 - Ubuntu update for libvirt - Secunia	web.archive.org, text/html	SECUNIA 62303
USN-2404-1: libvirt vulnerabilities | Ubuntu	Vendor Advisory, www.ubuntu.com, text/html	UBUNTU USN-2404-1
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities	security.gentoo.org, text/html	GENTOO GLSA-201412-04
openSUSE-SU-2014:1471-1: moderate: Security update for libvirt	lists.opensuse.org, text/html	SUSE openSUSE-SU-2014:1471
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	web.archive.org, text/html	SECUNIA 60895
Security Advisory SA60010 - SUSE update for libvirt - Secunia	web.archive.org	SECUNIA 60010

	text/html	
About Secunia Research | Flexera	web.archive.org text/html	SECUNIA 62058
Libvirt Security Notice: LSN-2014-0007	Patch Vendor Advisory security.libvirt.org text/xml	CONFIRM security.libvirt.org/2014/0007.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Libvirt	1.2.0	All	All	All
Application	Redhat	Libvirt	1.2.1	All	All	All
Application	Redhat	Libvirt	1.2.2	All	All	All
Application	Redhat	Libvirt	1.2.3	All	All	All
Application	Redhat	Libvirt	1.2.4	All	All	All
Application	Redhat	Libvirt	1.2.5	All	All	All
Application	Redhat	Libvirt	1.2.6	All	All	All
Application	Redhat	Libvirt	1.2.7	All	All	All
Application	Redhat	Libvirt	1.2.8	All	All	All
Application	Redhat	Libvirt	1.2.9	All	All	All
Application	Redhat	Libvirt	1.2.0	All	All	All
Application	Redhat	Libvirt	1.2.1	All	All	All
Application	Redhat	Libvirt	1.2.2	All	All	All
Application	Redhat	Libvirt	1.2.3	All	All	All
Application	Redhat	Libvirt	1.2.4	All	All	All
Application	Redhat	Libvirt	1.2.5	All	All	All
Application	Redhat	Libvirt	1.2.6	All	All	All
Application	Redhat	Libvirt	1.2.7	All	All	All
Application	Redhat	Libvirt	1.2.8	All	All	All
Application	Redhat	Libvirt	1.2.9	All	All	All
Application	Redhat	Libvirt	All	All	All	All

cpe:2.3:a:redhat:libvirt:1.2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.3:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.4:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.5:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.6:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.7:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.8:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.9:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.3:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.4:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.5:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.6:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.7:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.8:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.2.9:*:*:*:*:*:*:*

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→