CVE-2014-5177

Published on: 08/03/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:53 PM UTC

CVE-2014-5177

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

Certain versions of Opensuse from Opensuse contain the following vulnerability:

libvirt 1.0.0 through 1.2.x before 1.2.5, when fine grained access control is enabled, allows local users to read arbitrary files via a crafted XML document containing an XML external entity declaration in conjunction with an entity reference to the (1) virDomainDefineXML, (2) virNetworkCreateXML, (3) virNetworkDefineXML, (4) virStoragePoolCreateXML, (5) virStoragePoolDefineXML, (6) virStorageVolCreateXML, (7) virDomainCreateXML, (8) virNodeDeviceCreateXML, (9) virInterfaceDefineXML, (10) virStorageVolCreateXMLFrom, (11) virConnectDomainXMLFromNative, (12) virConnectDomainXMLToNative, (13) virSecretDefineXML, (14) virNWFilterDefineXML, (15) virDomainSnapshotCreateXML, (16) virDomainSaveImageDefineXML, (17) virDomainCreateXMLWithFiles, (18) virConnectCompareCPU, or (19) virConnectBaselineCPU API method, related to an XML External Entity (XXE) issue. NOTE: this issue was SPLIT from CVE-2014-0179 per ADT3 due to different affected versions of some vectors.

CVE-2014-5177 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 1.2 - LOW

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

CVE References

Description	Tags	Link
Libvirt Security Notice: LSN-2014-0003	Patch	CONFIRM

	Vendor Advisory security.libvirt.org text/xml	security.libvirt.org/2014/0003.html
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201412-04
USN-2366-1: libvirt vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2366-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0560
openSUSE-SU-2014:0650-1: moderate: libvirt: Fixed unsafe parsing of XML	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0650
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	web.archive.org text/html	SECUNIA 60895
openSUSE-SU-2014:0674-1: moderate: libvirt: Fix migration with QEMU 1.6	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0674
libvirt: Releases	libvirt.org text/xml	CONFIRM libvirt.org/news.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	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Application	Redhat	Enterprise Virtualization	3.0	All	All	All
Application	Redhat	Enterprise Virtualization	3.0	All	All	All
Application	Redhat	Libvirt	1.0.0	All	All	All
Application	Redhat	Libvirt	1.0.1	All	All	All
Application	Redhat	Libvirt	1.0.2	All	All	All

Application	Redhat	Libvirt	1.0.3	All	All	All
Application	Redhat	Libvirt	1.0.4	All	All	All
Application	Redhat	Libvirt	1.0.5	All	All	All
Application	Redhat	Libvirt	1.0.5.1	All	All	All
Application	Redhat	Libvirt	1.0.5.2	All	All	All
Application	Redhat	Libvirt	1.0.5.3	All	All	All
Application	Redhat	Libvirt	1.0.5.4	All	All	All
Application	Redhat	Libvirt	1.0.5.5	All	All	All
Application	Redhat	Libvirt	1.0.5.6	All	All	All
Application	Redhat	Libvirt	1.0.6	All	All	All
Application	Redhat	Libvirt	1.1.0	All	All	All
Application	Redhat	Libvirt	1.1.1	All	All	All
Application	Redhat	Libvirt	1.1.2	All	All	All
Application	Redhat	Libvirt	1.1.3	All	All	All
Application	Redhat	Libvirt	1.1.4	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	1.0.0	All	All	All
Application	Redhat	Libvirt	1.0.1	All	All	All
Application	Redhat	Libvirt	1.0.2	All	All	All
Application	Redhat	Libvirt	1.0.3	All	All	All
Application	Redhat	Libvirt	1.0.4	All	All	All
Application	Redhat	Libvirt	1.0.5	All	All	All
Application	Redhat	Libvirt	1.0.5.1	All	All	All
Application	Redhat	Libvirt	1.0.5.2	All	All	All
Application	Redhat	Libvirt	1.0.5.3	All	All	All
Application	Redhat	Libvirt	1.0.5.4	All	All	All
Application	Redhat	Libvirt	1.0.5.5	All	All	All
Application	Redhat	Libvirt	1.0.5.6	All	All	All
Application	Redhat	Libvirt	1.0.6	All	All	All
Application	Redhat	Libvirt	1.1.0	All	All	All
Application	Redhat	Libvirt	1.1.1	All	All	All
Application	Redhat	Libvirt	1.1.2	All	All	All

Application	Redhat	Libvirt	1.1.3	All	All	All
Application	Redhat	Libvirt	1.1.4	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

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_virtualization:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_virtualization:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.5.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:libvirt:1.1.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.3:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.4:*:*:*:*:*:*:*

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:1.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.4:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5.3:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5.4:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5.5:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.5.6:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.0.6:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.3:*:*:*:*:*:*:*

cpe:2.3:a:redhat:libvirt:1.1.4:*:*:*:*:*:*:*

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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→