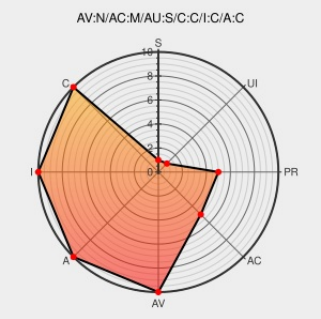
CVE-2013-4401

Published on: 11/02/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:46:00 AM UTC

CVE-2013-4401

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



Certain versions of Libvirt from Redhat contain the following vulnerability:

The virConnectDomainXMLToNative API function in libvirt 1.1.0 through 1.1.3 checks for the connect:read permission instead of the connect:write permission, which allows attackers to gain domain:write privileges and execute Qemu binaries via crafted XML. NOTE: some of these details are obtained from third party information.

CVE-2013-4401 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
libvirt.org Git - libvirt.git/commit	web.archive.org text/xml Inactive Link Not Archived	MISC libvirt.org/git/?p=libvirt.git%3Ba=commit%3Bh=57687fd6bf7f6e1b3662c52f3f26c06ab19dc96c
1015259 – (CVE-2013-4401) CVE-2013-4401 libvirt: unintended API access due to incorrect permissions checks	Patch bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1015259
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201412-04
libvirt: Wiki: Maintenance Releases	wiki.libvirt.org text/html	CONFIRM wiki.libvirt.org/page/Maintenance_Releases

USN-2026-1: libvirt vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2026-1
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	web.archive.org text/html	SECUNIA 60895
libvirt API Access Control Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1029241
Security Advisory SA55210 - libvirt Privilege Escalation and Security Bypass Vulnerabilities - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 55210

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	1.1.0	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	1.1.0	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

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:1.1.0:*:*:*:*:*:*:*

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→