



CVE-2013-6456

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-6456
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-15 23:55:00 UTC
Updated	2023-02-13 00:29:00 UTC
Description	The LXC driver (lxc/lxc_driver.c) in libvirt 1.0.1 through 1.2.1 allows local users to (1) delete arbitrary host devices via the vi

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	20	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	1.0.1	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

References						
Reference					Source	Link
openSUSE-SU-2014:0593-1: moderate: libvirt					SUSE	lists
#732394 - libvirt-bin: CVE-2013-6456: virsh shutdown does not handle symlinks correctly for LXC - Debian Bug report logs					MISC	bug
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities					GENTOO	sec
libvirt.org Git - libvirt.git/commit					MISC	libv
libvirt.org Git - libvirt.git/commit					CONFIRM	libv
About Secunia Research Flexera					SECUNIA	sec
Security Advisory SA60895 - Gentoo update for libvirt - Secunia					SECUNIA	sec
Security Advisory SA56187 - libvirt LXC Devices Hotplug Handling Security Issues - Secunia					SECUNIA	sec
[SECURITY] Fedora 20 Update: libvirt-1.1.3.4-1.fc20					FEDORA	lists
libvirt.org Git - libvirt.git/commit					MISC	

libvirt Unsafe Paths Usage Symlink Multiple Security Vulnerabilities	BID	www
libvirt: Releases	CONFIRM	libv
Libvirt Security Notice: LSN-2013-0018	CONFIRM	sec
Bug 1045643 – CVE-2013-6456 libvirt: vulnerability in virInitctlSetRunLevel [rhel-7.0]	CONFIRM	bug
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)