CVE-2014-0028

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-0028
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-24 18:55:00 UTC
Updated	2015-01-03 02:08:00 UTC
Description	libvirt 1.1.1 through 1.2.0 allows context-dependent attackers to bypass the domain:getattr and connect:search_domains re

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.1.1	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

References

Reference	Source	Link	Tag
USN-2093-1: libvirt vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com	
[libvirt] [PATCH 0/4] CVE-2014-0028: domain events vs. ACL filtering	MLIST	www.redhat.com	
Gentoo Linux Documentation -- libvirt: Multiple vulnerabilities	GENTOO	security.gentoo.org	
Security Advisory SA60895 - Gentoo update for libvirt - Secunia	SECUNIA	secunia.com	

libvirt: Releases	CONFIRM	libvirt.org	
openSUSE-SU-2014:0268-1: moderate: update for libvirt	SUSE	lists.opensuse.org	
1048637 – (CVE-2014-0028) CVE-2014-0028 libvirt: event registration bypasses domain:getattr ACL	CONFIRM	bugzilla.redhat.com	Ver
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

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 registred 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**