CVE-2012-4539

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

Summary

CVE	CVE-2012-4539
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-21 23:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Xen 4.0 through 4.2, when running 32-bit x86 PV guests on 64-bit hypervisors, allows local guest OS administrators to caus

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All

Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All

References

Reference	Source	Link
Security Advisory SA51200 - Xen Multiple Denial of Service Vulnerabilities - Secunia	SECUNIA	secunia.co
[security-announce] SUSE-SU-2012:1487-1: important: Security update for	SUSE	lists.opensu
[security-announce] SUSE-SU-2012:1615-1: important: Security update for	SUSE	lists.opensu
Security Advisory SA51352 - SUSE update for libvirt - Secunia	SECUNIA	secunia.co
Xen Multiple Denial of Service Vulnerabilities	BID	www.secur
[security-announce] openSUSE-SU-2012:1572-1: important: XEN: security an	SUSE	lists.opensu
[security-announce] openSUSE-SU-2012:1685-1: important: xen to fix vario	SUSE	lists.opensu
oss-security - Xen Security Advisory 24 (CVE-2012-4539) - Grant table hypercall infinite loop DoS vulnerability	MLIST	www.openv
87305	OSVDB	www.osvdb
Security Advisory SA51468 - Debian update for xen - Secunia	SECUNIA	secunia.co
Security Advisory SA51413 - SUSE update for xen - Secunia	SECUNIA	secunia.co
Security Advisory SA51324 - SUSE update for xen - Secunia	SECUNIA	secunia.co
Security Advisory SA55082 - Gentoo update for xen - Secunia	SECUNIA	secunia.co
Xen Grant Table Hypercall Infinite Loop Lets Local Guest Administrative Users Deny Service - SecurityTracker	SECTRACK	www.secur
[Xen-announce] Xen Security Advisory 24 (CVE-2012-4539) - Grant table hypercall infinite loop DoS vulnerability	MLIST	lists.xen.or
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	GENTOO	security.ge
[security-announce] openSUSE-SU-2012:1573-1: important: XEN: security an	SUSE	lists.opensu
[security-announce] SUSE-SU-2012:1486-1: important: Security update for	SUSE	lists.opensu
IBM X-Force Exchange	XF	exchange.x
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	GENTOO	security.ge
[security-announce] SUSE-SU-2014:0446-1: important: Security update for	SUSE	lists.opensu
Debian -- Security Information -- DSA-2582-1 xen	DEBIAN	www.debia
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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