CVE-2012-5513

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

Summary

CVE	CVE-2012-5513
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-13 11:53:00 UTC
Updated	2023-02-13 00:26:00 UTC
Description	The XENMEM_exchange handler in Xen 4.2 and earlier does not properly check the memory address, which allows local P

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	3.0.2	All	All	All
Operating System	Xen	Xen	3.0.3	All	All	All
Operating System	Xen	Xen	3.0.4	All	All	All
Operating System	Xen	Xen	3.1.3	All	All	All
Operating System	Xen	Xen	3.1.4	All	All	All
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	All	All	All
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	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	3.0.2	All	All	All
Operating System	Xen	Xen	3.0.3	All	All	All
Operating System	Xen	Xen	3.0.4	All	All	All
Operating System	Xen	Xen	3.1.3	All	All	All
Operating System	Xen	Xen	3.1.4	All	All	All
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	All	All	All
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	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	All	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rhn.redhat
About Secunia Research | Flexera	SECUNIA	secunia.co
openSUSE-SU-2013:0636-1: moderate: xen: security and bugfix update	SUSE	lists.opens
[security-announce] SUSE-SU-2012:1615-1: important: Security update for	SUSE	lists.opens
Bug 877391 – CVE-2012-5513 kernel: xen: XENMEM_exchange may overwrite hypervisor memory	MISC	bugzilla.re
Xen 'XENMEM_exchange' Local Privilege Escalation Vulnerability	BID	www.secu
Citrix XenServer Multiple Security Updates	CONFIRM	support.cit
About Secunia Research | Flexera	SECUNIA	secunia.co
openSUSE-SU-2013:0637-1: moderate: xen: security and bugfix update	SUSE	lists.opens
Security Advisory SA51495 - SUSE update for xen - Secunia	SECUNIA	secunia.co
[security-announce] SUSE-SU-2012:1606-1: important: Security update for	SUSE	lists.opens
Red Hat Customer Portal	MISC	access.red
[security-announce] openSUSE-SU-2012:1685-1: important: xen to fix vario	SUSE	lists.opens
Security Advisory SA51468 - Debian update for xen - Secunia	SECUNIA	secunia.co
oss-security - Xen Security Advisory 29 (CVE-2012-5513) - XENMEM_exchange may overwrite hypervisor memory	MLIST	www.open
Security Advisory SA55082 - Gentoo update for xen - Secunia	SECUNIA	secunia.co
About Secunia Research | Flexera	SECUNIA	secunia.co
[security-announce] openSUSE-SU-2013:0133-1: important: xen to fix vario	SUSE	lists.opens
[security-announce] SUSE-SU-2014:0470-1: important: Security update for	SUSE	lists.opens
[security-announce] openSUSE-SU-2012:1687-1: important: xen to fix vario	SUSE	lists.opens
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	GENTOO	security.ge
access.redhat.com | CVE-2012-5513	MISC	access.red
88131	OSVDB	www.osvd
[security-announce] SUSE-SU-2014:0446-1: important: Security update for	SUSE	lists.opens
IBM X-Force Exchange	XF	exchange.
Debian -- Security Information -- DSA-2582-1 xen	DEBIAN	www.debia
CVE Program record	CVE.ORG	www.cve.c
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.