



CVE-2012-5511

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

Summary

CVE	CVE-2012-5511
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-13 11:53:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Stack-based buffer overflow in the dirty video RAM tracking functionality in Xen 3.4 through 4.1 allows local HVM guest OS

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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

References						
Reference					Source	Link
About Secunia Research Flexera					SECUNIA	secunia.com
openSUSE-SU-2013:0636-1: moderate: xen: security and bugfix update					SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2012:1615-1: important: Security update for					SUSE	lists.opensuse.org
oss-security - Xen Security Advisory 27 (CVE-2012-5511) - several HVM operations do not validate the range of their inputs					MLIST	www.openwall.com
Debian -- Security Information -- DSA-2636-2 xen					DEBIAN	www.debian.org
Citrix XenServer Multiple Security Updates					CONFIRM	support.citrix.com
About Secunia Research Flexera					SECUNIA	secunia.com
openSUSE-SU-2013:0637-1: moderate: xen: security and bugfix update					SUSE	lists.opensuse.org
Xen Bitmap Local Denial of Service Vulnerability					BID	www.bidsa.org
[security-announce] openSUSE-SU-2012:1685-1: important: xen to fix vario					SUSE	lists.opensuse.org
88129					OSVDB	www.osvdb.org
Security Advisory SA55082 - Gentoo update for xen - Secunia					SECUNIA	secunia.com
About Secunia Research Flexera					SECUNIA	secunia.com
[security-announce] openSUSE-SU-2013:0133-1: important: xen to fix vario					SUSE	lists.opensuse.org
[security-announce] openSUSE-SU-2012:1687-1: important: xen to fix vario					SUSE	lists.opensuse.org
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities					GENTOO	security.gentoo.org
[security-announce] SUSE-SU-2014:0446-1: important: Security update for					SUSE	lists.opensuse.org
IBM X-Force Exchange					XF	exchange.xforce.ibmcloud.com
CVE Program record					CVE.ORG	www.cve.org
NVD vulnerability detail					NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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