CVE-2012-0217

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2012-0217
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-12 22:55:00 UTC
Updated	2020-09-28 12:58:00 UTC
Description	The x86-64 kernel system-call functionality in Xen 4.1.2 and earlier, as used in Citrix XenServer 6.0.2 and earlier and other

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Xenserver	6.0	All	All	All
Application	Citrix	Xenserver	6.0	All	All	All
Application	Citrix	Xenserver	All	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Illumos	Illumos	All	All	All	All
Operating System	Joyent	Smartos	All	All	All	All
Operating System	Microsoft	Windows 7	All	All	x64	All
Operating System	Microsoft	Windows 7	All	sp1	x64	All
Operating System	Microsoft	Windows 7	All	All	x64	All
Operating System	Microsoft	Windows 7	All	sp1	x64	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Server 2008	r2	All	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Netbsd	Netbsd	All	beta	All	All

Operating System	Sun	Sunos	All	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	4.0.0	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	All	All	All	All

References

Reference	Source	L
Citrix XenServer Multiple Security Updates	CONFIRM	s
Microsoft Security Bulletin MS12-042 - Important | Microsoft Docs	MS	d
Repository / Oval Repository	OVAL	o
[Xen-devel] Security vulnerability process, and CVE-2012-0217	MLIST	lis
SmartOS Change Log - SmartOS Documentation - SmartOS Wiki	CONFIRM	w
Bug 813428 – CVE-2012-0217 kernel: x86-64: avoid sysret to non-canonical address	CONFIRM	b
FreeBSD-SA-12:04	FREEBSD	s
illumos gate - Bug #2873: sysretq doesn't properly handle non-canonical addresses - illumos.org	CONFIRM	w
Vulnerability Note VU#649219 - SYSRET 64-bit operating system privilege escalation vulnerability on Intel CPU hardware	CERT-VN	w
US-CERT Alert TA12-164A -- Microsoft Updates for Multiple Vulnerabilities	CERT	w
NetBSD-SA2012-003	NETBSD	ft
Debian -- Security Information -- DSA-2508-1 kfreebsd-8	DEBIAN	w
The Intel SYSRET privilege escalation – blog.xen.org	CONFIRM	b
Oracle Critical Patch Update - October 2012	CONFIRM	w
Support / Security / Advisories / / MDVSA-2013:150 | Mandriva	MANDRIVA	w
[Xen-announce] Xen Security Advisory 7 (CVE-2012-0217) - PV privilege escalation	MLIST	lis

Security Advisory SA55082 - Gentoo update for xen - Secunia	SECUNIA	s
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	GENTOO	s
FreeBSD - Intel SYSRET Privilege Escalation (Metasploit) - FreeBSD_x86-64 local Exploit	EXPLOIT-DB	w
illumos» Blog Archive » Patch for illumos CERT Vulnerability	CONFIRM	b
SmartOS News: June 15, 2012 – SmartOS.org	CONFIRM	s
Debian -- Security Information -- DSA-2501-1 xen	DEBIAN	w
FreeBSD Intel SYSRET Kernel Privilege Escalation Exploit	EXPLOIT-DB	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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