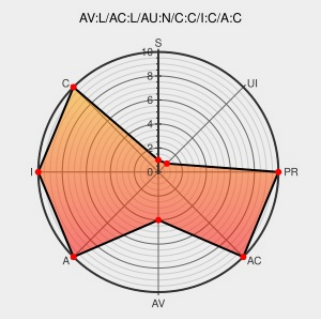
CVE-2015-7835

Published on: 10/30/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

CVE-2015-7835

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xen from Xen contain the following vulnerability:

The mod_l2_entry function in arch/x86/mm.c in Xen 3.4 through 4.6.x does not properly validate level 2 page table entries, which allows local PV guest administrators to gain privileges via a crafted superpage mapping.

CVE-2015-7835 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Xen CVE-2015-7835 Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 77366
Debian -- Security Information -- DSA-3390-1 xen	www.debian.org Depreciated Link text/html	DEBIAN DSA-3390
qubes-secpack/qsb-022-2015.txt at master · QubesOS/qubes-secpack · GitHub	Vendor Advisory github.com text/html	MISC github.com/QubesOS/qubes-secpack/blob/master/QSBs/qsb-022-2015.txt
404 - Page not found	support.citrix.com text/html	CONFIRM support.citrix.com/article/CTX202404
[SECURITY] Fedora 21 Update: xen-4.4.3-7.fc21	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-242be2c240

openSUSE-SU-2015:1965-1: moderate: Security update for xen	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1965
[SECURITY] Fedora 23 Update: xen-4.5.1-14.fc23	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-a931b02be2
XSA-148 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-148.html
Xen Page Table Validation Bypass Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034032
openSUSE-SU-2015:2250-1: moderate: Security update for xen	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2250
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201604-03
[SECURITY] Fedora 22 Update: xen-4.5.1-14.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-6f6b79efe2

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	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	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.1	-	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.6.0	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
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	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All

Operating System	Xen	Xen	4.4.1	-	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All

cpe:2.3:o:xen:xen:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.1:-:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.1:-:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→