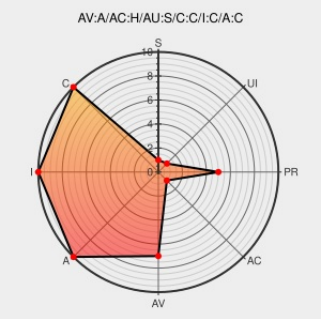
CVE-2013-4329

Published on: 09/12/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:13 AM UTC

CVE-2013-4329

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



Certain versions of Xen from Xen contain the following vulnerability:

The xenlight library (libxl) in Xen 4.0.x through 4.2.x, when IOMMU is disabled, provides access to a busmastering-capable PCI passthrough device before the IOMMU setup is complete, which allows local HVM guest domains to gain privileges or cause a denial of service via a DMA instruction.

CVE-2013-4329 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3006-1 xen	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3006
Gentoo Linux Documentation -- Xen: Multiple Vunlerabilities	security.gentoo.org, text/html	GENTOO GLSA-201407-03
Xen project Mailing List	Patch, lists.xen.org, text/html	MLIST [Xen-devel] 20130701 [PATCH] libxl: suppress device assignment to HVM guest when there is no IOMMU
[security-announce] SUSE-SU-2014:0446-1: important: Security update for	lists.opensuse.org, text/html	SUSE SUSE-SU-2014:0446
oss-security - Re: Xen Security Advisory 61 - libxl partially sets up HVM passthrough even with disabled iommu	www.openwall.com, text/html	MLIST [oss-security] 20130910 Re: Xen Security Advisory 61 - libxl partially sets up HVM passthrough even with disabled iommu

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	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	4.2.0	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	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All

System

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	4.2.0	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

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:4.2.0:*:*:*:*:*:*:*:

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:4.0.0:*:*:*:*:*:*:*:

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:4.2.0:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→