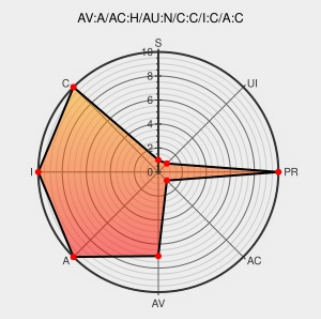
CVE-2013-6400

Published on: 12/13/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

CVE-2013-6400

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



Certain versions of Xen from Xen contain the following vulnerability:

Xen 4.2.x and 4.3.x, when using Intel VT-d and a PCI device has been assigned, does not clear the flag that suppresses IOMMU TLB flushes when unspecified errors occur, which causes the TLB entries to not be flushed and allows local guest administrators to cause a denial of service (host crash) or gain privileges via unspecified vectors.

CVE-2013-6400 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2014:0373-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2014:0373
oss-security - Xen Security Advisory 80 (CVE-2013-6400) - IOMMU TLB flushing may be inadvertently suppressed	www.openwall.com text/html	MLIST [oss-security] 20131210 Xen Security Advisory 80 (CVE-2013-6400) - IOMMU TLB flushing may be inadvertently suppressed
Xen project Mailing List	lists.xen.org text/html	MLIST [Xen-announce] 20131210 Xen Security Advisory 80 (CVE-2013-6400) - IOMMU TLB flushing may be inadvertently suppressed
[SECURITY] Fedora 19 Update: xen-4.2.3-12.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-23457
[SECURITY] Fedora 18 Update: xen-4.2.3-12.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-23466

Gentoo Linux Documentation -- Xen: Multiple Vunlerabilities	security.gentoo.org text/html	GENTOO GLSA-201407-03
Security Advisory SA55932 - Xen IOMMU TLB Flushing Suppress Flag Privilege Escalation Vulnerability - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 55932
Xen IOMMU TLB Flush Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1029468

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	4.2.0	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	4.2.0	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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→