



CVE-2013-6375

Published on: 11/23/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

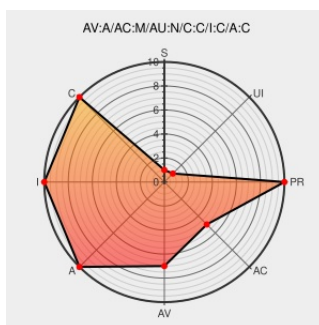
CVE-2013-6375

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Opensuse](#) from [Opensuse](#) contain the following vulnerability:

Xen 4.2.x and 4.3.x, when using Intel VT-d for PCI passthrough, does not properly flush the TLB after clearing a present translation table entry, which allows local guest administrators to cause a denial of service or gain privileges via unspecified vectors related to an "inverted boolean parameter."

CVE-2013-6375 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.9 - HIGH**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Xen TLB Flushing Error Lets Local Users on the Guest Operating System Deny Service or Gain Elevated Privileges on the Host System - SecurityTracker

[Third Party Advisory](#)
[VDB Entry](#)
www.securitytracker.com
[text/html](#)

[SECTrack 1029369](#)

oss-security - Re: Xen Security Advisory 78 - Insufficient TLB flushing in VT-d (iommu) code

[Mailing List](#)
[Third Party Advisory](#)
www.openwall.com
[text/html](#)

[MLIST \[oss-security\] 20131121 Re: Xen Security Advisory 78 - Insufficient TLB flushing in VT-d \(iommu\) code](#)

openSUSE-SU-2013:1876-1: moderate: xen: security and bugfix update

[Third Party Advisory](#)
lists.opensuse.org
[text/html](#)

[SUSE openSUSE-SU-2013:1876](#)

Gentoo Linux Documentation -- Xen: Multiple Vulnerabilities

security.gentoo.org

[GENTOO GLSA-201407-03](#)

[text/html](#)

oss-security - Xen Security Advisory 78 - Insufficient TLB flushing in VT-d (iommu) code

[Mailing List](#)[Third Party Advisory](#)[www.openwall.com](#)[text/html](#)

 [MLIST \[oss-security\] 20131120 Xen Security Advisory 78 - Insufficient TLB flushing in VT-d \(iommu\) code](#)

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

Exploit/POC from Github

Xen 4.2.x and 4.3.x, when using Intel VT-d for PCI passthrough, does not properly flush the TLB after clearing a pres...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	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	4.2.1	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:opensuse:opensuse:13.1:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:
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:4.2.1:*:*:*:*:*:
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→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

CVE.report and Source URL Uptime Status status.cve.report