



CVE-2016-5242

Published on: 06/07/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:09 PM UTC

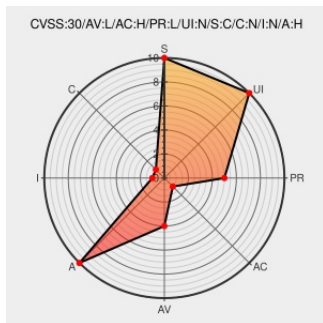
CVE-2016-5242

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The p2m_takedown function in arch/arm/p2m.c in Xen 4.4.x through 4.6.x allows local guest OS users with access to the driver domain to cause a denial of service (NULL pointer dereference and host OS crash) by creating concurrent domains and holding references to them, related to VMID exhaustion.

CVE-2016-5242 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.7 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
XSA-181 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-181.html
Xen VMID Resource Exhaustion Bug Lets Local Domain Drivers Cause Denial of	www.securitytracker.com	SECTRACK 1036035

Service Conditions on the Host System - SecurityTracker

Xen VMID Exhaustion Denial of Service Vulnerability

cve.report (archive)

text/html

BID 91015

Debian -- Security Information -- DSA-3633-1 xen

www.debian.org

Deprecated Link

text/html

DEBIAN DSA-3633

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	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.1	All	All	All
Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.4.4	All	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	4.5.2	All	All	All
Operating System	Xen	Xen	4.5.3	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.1	All	All	All

Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.4.4	All	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	4.5.2	All	All	All
Operating System	Xen	Xen	4.5.3	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.1	All	All	All
cpe:2.3:o:xen:xen:4.4.0:*****:						
cpe:2.3:o:xen:xen:4.4.0:rc1:*****:						
cpe:2.3:o:xen:xen:4.4.1:*****:						
cpe:2.3:o:xen:xen:4.4.2:*****:						
cpe:2.3:o:xen:xen:4.4.3:*****:						
cpe:2.3:o:xen:xen:4.4.4:*****:						
cpe:2.3:o:xen:xen:4.5.0:*****:						
cpe:2.3:o:xen:xen:4.5.1:*****:						
cpe:2.3:o:xen:xen:4.5.2:*****:						
cpe:2.3:o:xen:xen:4.5.3:*****:						
cpe:2.3:o:xen:xen:4.6.0:*****:						
cpe:2.3:o:xen:xen:4.6.1:*****:						
cpe:2.3:o:xen:xen:4.4.0:*****:						
cpe:2.3:o:xen:xen:4.4.0:rc1:*****:						
cpe:2.3:o:xen:xen:4.4.1:*****:						
cpe:2.3:o:xen:xen:4.4.2:*****:						
cpe:2.3:o:xen:xen:4.4.3:*****:						

cpe:2.3:o:xen:xen:4.4.4:*****:
cpe:2.3:o:xen:xen:4.5.0:*****:
cpe:2.3:o:xen:xen:4.5.1:*****:
cpe:2.3:o:xen:xen:4.5.2:*****:
cpe:2.3:o:xen:xen:4.5.3:*****:
cpe:2.3:o:xen:xen:4.6.0:*****:
cpe:2.3:o:xen:xen:4.6.1:*****:

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](#)