

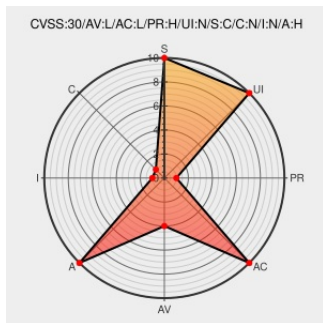


CVE-2017-15596

Published on: 10/18/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15596

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

An issue was discovered in Xen 4.4.x through 4.9.x allowing ARM guest OS users to cause a denial of service (prevent physical CPU usage) because of lock mishandling upon detection of an add-to-physmap error.

CVE-2017-15596 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6 - MEDIUM**

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

CVSS2 Score: **4.9 - MEDIUM**

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

CVE References

Description	Tags	Link
XSA-235 - Xen Security Advisories	Mitigation Patch Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-235.html

Xen Multiple Flaws on x86 Systems Let Local Guest System Users Obtain Memory Contents and Potentially Sensitive Information, Deny Service on the Host System, and Gain Elevated Privileges on the Host System - SecurityTracker

Third Party Advisory

SECTrack 1039568

VDB Entry

www.securitytracker.com

text/html

Debian -- Security Information -- DSA-3969-1 xen

www.debian.org

DEBIAN DSA-3969

Deprecated Link

text/html

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	4.4.0	rc2	All	All
Operating System	Xen	Xen	4.4.0	rc3	All	All
Operating System	Xen	Xen	4.4.0	rc4	All	All
Operating System	Xen	Xen	4.4.0	rc5	All	All
Operating System	Xen	Xen	4.4.0	rc6	All	All
Operating System	Xen	Xen	4.4.1	All	All	All
Operating System	Xen	Xen	4.4.1	rc1	All	All
Operating System	Xen	Xen	4.4.1	rc2	All	All
Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.2	rc1	All	All
Operating System	Xen	Xen	4.4.2	rc2	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.4.3	rc1	All	All

System						
Operating System	Xen	Xen	4.4.4	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.0	rc1	All	All
Operating System	Xen	Xen	4.5.0	rc2	All	All
Operating System	Xen	Xen	4.5.0	rc3	All	All
Operating System	Xen	Xen	4.5.0	rc4	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.1	rc1	All	All
Operating System	Xen	Xen	4.5.1	rc2	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	4.5.4	All	All	All
Operating System	Xen	Xen	4.5.5	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.0	rc1	All	All
Operating System	Xen	Xen	4.6.0	rc2	All	All
Operating System	Xen	Xen	4.6.0	rc3	All	All
Operating System	Xen	Xen	4.6.0	rc4	All	All
Operating System	Xen	Xen	4.6.0	rc5	All	All
Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.6.2	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.6.4	All	All	All

System						
Operating System	Xen	Xen	4.6.5	All	All	All
Operating System	Xen	Xen	4.6.6	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
Operating System	Xen	Xen	4.7.0	rc1	All	All
Operating System	Xen	Xen	4.7.0	rc2	All	All
Operating System	Xen	Xen	4.7.0	rc3	All	All
Operating System	Xen	Xen	4.7.0	rc4	All	All
Operating System	Xen	Xen	4.7.0	rc5	All	All
Operating System	Xen	Xen	4.7.0	rc6	All	All
Operating System	Xen	Xen	4.7.1	All	All	All
Operating System	Xen	Xen	4.7.2	All	All	All
Operating System	Xen	Xen	4.7.3	All	All	All
Operating System	Xen	Xen	4.8.0	All	All	All
Operating System	Xen	Xen	4.8.0	rc1	All	All
Operating System	Xen	Xen	4.8.0	rc2	All	All
Operating System	Xen	Xen	4.8.0	rc3	All	All
Operating System	Xen	Xen	4.8.0	rc4	All	All
Operating System	Xen	Xen	4.8.0	rc5	All	All
Operating System	Xen	Xen	4.8.0	rc6	All	All
Operating System	Xen	Xen	4.8.0	rc7	All	All
Operating System	Xen	Xen	4.8.0	rc8	All	All
Operating System	Xen	Xen	4.8.1	All	All	All
Operating	Xen	Xen	4.8.2	All	All	All

System						
Operating System	Xen	Xen	4.9.0	All	All	All
Operating System	Xen	Xen	4.9.0	rc1	All	All
Operating System	Xen	Xen	4.9.0	rc1.1	All	All
Operating System	Xen	Xen	4.9.0	rc1.2	All	All
Operating System	Xen	Xen	4.9.0	rc2	All	All
Operating System	Xen	Xen	4.9.0	rc3	All	All
Operating System	Xen	Xen	4.9.0	rc4	All	All
Operating System	Xen	Xen	4.9.0	rc5	All	All
Operating System	Xen	Xen	4.9.0	rc6	All	All
Operating System	Xen	Xen	4.9.0	rc7	All	All
Operating System	Xen	Xen	4.9.0	rc8	All	All
Operating System	Xen	Xen	4.9.0	rc9	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	4.4.0	rc2	All	All
Operating System	Xen	Xen	4.4.0	rc3	All	All
Operating System	Xen	Xen	4.4.0	rc4	All	All
Operating System	Xen	Xen	4.4.0	rc5	All	All
Operating System	Xen	Xen	4.4.0	rc6	All	All
Operating System	Xen	Xen	4.4.1	All	All	All
Operating System	Xen	Xen	4.4.1	rc1	All	All
Operating System	Xen	Xen	4.4.1	rc2	All	All
Operating	Xen	Xen	4.4.2	All	All	All

System						
Operating System	Xen	Xen	4.4.2	rc1	All	All
Operating System	Xen	Xen	4.4.2	rc2	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.4.3	rc1	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	4.5.0	rc1	All	All
Operating System	Xen	Xen	4.5.0	rc2	All	All
Operating System	Xen	Xen	4.5.0	rc3	All	All
Operating System	Xen	Xen	4.5.0	rc4	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.1	rc1	All	All
Operating System	Xen	Xen	4.5.1	rc2	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	4.5.4	All	All	All
Operating System	Xen	Xen	4.5.5	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.0	rc1	All	All
Operating System	Xen	Xen	4.6.0	rc2	All	All
Operating System	Xen	Xen	4.6.0	rc3	All	All
Operating System	Xen	Xen	4.6.0	rc4	All	All
Operating	Xen	Xen	4.6.0	rc5	All	All

System						
Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.6.2	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.6.4	All	All	All
Operating System	Xen	Xen	4.6.5	All	All	All
Operating System	Xen	Xen	4.6.6	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
Operating System	Xen	Xen	4.7.0	rc1	All	All
Operating System	Xen	Xen	4.7.0	rc2	All	All
Operating System	Xen	Xen	4.7.0	rc3	All	All
Operating System	Xen	Xen	4.7.0	rc4	All	All
Operating System	Xen	Xen	4.7.0	rc5	All	All
Operating System	Xen	Xen	4.7.0	rc6	All	All
Operating System	Xen	Xen	4.7.1	All	All	All
Operating System	Xen	Xen	4.7.2	All	All	All
Operating System	Xen	Xen	4.7.3	All	All	All
Operating System	Xen	Xen	4.8.0	All	All	All
Operating System	Xen	Xen	4.8.0	rc1	All	All
Operating System	Xen	Xen	4.8.0	rc2	All	All
Operating System	Xen	Xen	4.8.0	rc3	All	All
Operating System	Xen	Xen	4.8.0	rc4	All	All
Operating System	Xen	Xen	4.8.0	rc5	All	All
Operating System	Xen	Xen	4.8.0	rc6	All	All

Operating System	Xen	Xen				
Operating System	Xen	Xen	4.8.0	rc7	All	All
Operating System	Xen	Xen	4.8.0	rc8	All	All
Operating System	Xen	Xen	4.8.1	All	All	All
Operating System	Xen	Xen	4.8.2	All	All	All
Operating System	Xen	Xen	4.9.0	All	All	All
Operating System	Xen	Xen	4.9.0	rc1	All	All
Operating System	Xen	Xen	4.9.0	rc1.1	All	All
Operating System	Xen	Xen	4.9.0	rc1.2	All	All
Operating System	Xen	Xen	4.9.0	rc2	All	All
Operating System	Xen	Xen	4.9.0	rc3	All	All
Operating System	Xen	Xen	4.9.0	rc4	All	All
Operating System	Xen	Xen	4.9.0	rc5	All	All
Operating System	Xen	Xen	4.9.0	rc6	All	All
Operating System	Xen	Xen	4.9.0	rc7	All	All
Operating System	Xen	Xen	4.9.0	rc8	All	All
Operating System	Xen	Xen	4.9.0	rc9	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:4.4.0:rc2:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.4.0:rc3:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.4.0:rc4:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.4.0:rc5:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.4.0:rc6:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.4.1:*:*:*:*:*:						

cpe:2.3:o:xen:xen:4.4.1:rc1:*****:
cpe:2.3:o:xen:xen:4.4.1:rc2:*****:
cpe:2.3:o:xen:xen:4.4.2:*****:
cpe:2.3:o:xen:xen:4.4.2:rc1:*****:
cpe:2.3:o:xen:xen:4.4.2:rc2:*****:
cpe:2.3:o:xen:xen:4.4.3:*****:
cpe:2.3:o:xen:xen:4.4.3:rc1:*****:
cpe:2.3:o:xen:xen:4.4.4:*****:
cpe:2.3:o:xen:xen:4.5.0:*****:
cpe:2.3:o:xen:xen:4.5.0:rc1:*****:
cpe:2.3:o:xen:xen:4.5.0:rc2:*****:
cpe:2.3:o:xen:xen:4.5.0:rc3:*****:
cpe:2.3:o:xen:xen:4.5.0:rc4:*****:
cpe:2.3:o:xen:xen:4.5.1:*****:
cpe:2.3:o:xen:xen:4.5.1:rc1:*****:
cpe:2.3:o:xen:xen:4.5.1:rc2:*****:
cpe:2.3:o:xen:xen:4.5.2:*****:
cpe:2.3:o:xen:xen:4.5.3:*****:
cpe:2.3:o:xen:xen:4.5.4:*****:
cpe:2.3:o:xen:xen:4.5.5:*****:
cpe:2.3:o:xen:xen:4.6.0:*****:
cpe:2.3:o:xen:xen:4.6.0:rc1:*****:
cpe:2.3:o:xen:xen:4.6.0:rc2:*****:
cpe:2.3:o:xen:xen:4.6.0:rc3:*****:
cpe:2.3:o:xen:xen:4.6.0:rc4:*****:
cpe:2.3:o:xen:xen:4.6.0:rc5:*****:
cpe:2.3:o:xen:xen:4.6.1:*****:
cpe:2.3:o:xen:xen:4.6.2:*****:

cpe:2.3:o:xen:xen:4.6.3:*****:
cpe:2.3:o:xen:xen:4.6.4:*****:
cpe:2.3:o:xen:xen:4.6.5:*****:
cpe:2.3:o:xen:xen:4.6.6:*****:
cpe:2.3:o:xen:xen:4.7.0:*****:
cpe:2.3:o:xen:xen:4.7.0:rc1:*****:
cpe:2.3:o:xen:xen:4.7.0:rc2:*****:
cpe:2.3:o:xen:xen:4.7.0:rc3:*****:
cpe:2.3:o:xen:xen:4.7.0:rc4:*****:
cpe:2.3:o:xen:xen:4.7.0:rc5:*****:
cpe:2.3:o:xen:xen:4.7.0:rc6:*****:
cpe:2.3:o:xen:xen:4.7.1:*****:
cpe:2.3:o:xen:xen:4.7.2:*****:
cpe:2.3:o:xen:xen:4.7.3:*****:
cpe:2.3:o:xen:xen:4.8.0:*****:
cpe:2.3:o:xen:xen:4.8.0:rc1:*****:
cpe:2.3:o:xen:xen:4.8.0:rc2:*****:
cpe:2.3:o:xen:xen:4.8.0:rc3:*****:
cpe:2.3:o:xen:xen:4.8.0:rc4:*****:
cpe:2.3:o:xen:xen:4.8.0:rc5:*****:
cpe:2.3:o:xen:xen:4.8.0:rc6:*****:
cpe:2.3:o:xen:xen:4.8.0:rc7:*****:
cpe:2.3:o:xen:xen:4.8.0:rc8:*****:
cpe:2.3:o:xen:xen:4.8.1:*****:
cpe:2.3:o:xen:xen:4.8.2:*****:
cpe:2.3:o:xen:xen:4.9.0:*****:
cpe:2.3:o:xen:xen:4.9.0:rc1:*****:
cpe:2.3:o:xen:xen:4.9.0:rc1.1:*****:
cpe:2.3:o:xen:xen:4.9.0:rc1.2:*****:

cpe:2.3:o:xen:xen:4.9.0:rc2:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc3:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc4:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc5:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc6:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc7:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc8:~::~~::
cpe:2.3:o:xen:xen:4.9.0:rc9:~::~~::
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:4.4.0:rc2:~::~~::
cpe:2.3:o:xen:xen:4.4.0:rc3:~::~~::
cpe:2.3:o:xen:xen:4.4.0:rc4:~::~~::
cpe:2.3:o:xen:xen:4.4.0:rc5:~::~~::
cpe:2.3:o:xen:xen:4.4.0:rc6:~::~~::
cpe:2.3:o:xen:xen:4.4.1:~::~~::
cpe:2.3:o:xen:xen:4.4.1:rc1:~::~~::
cpe:2.3:o:xen:xen:4.4.1:rc2:~::~~::
cpe:2.3:o:xen:xen:4.4.2:~::~~::
cpe:2.3:o:xen:xen:4.4.2:rc1:~::~~::
cpe:2.3:o:xen:xen:4.4.2:rc2:~::~~::
cpe:2.3:o:xen:xen:4.4.3:~::~~::
cpe:2.3:o:xen:xen:4.4.3:rc1:~::~~::
cpe:2.3:o:xen:xen:4.4.4:~::~~::
cpe:2.3:o:xen:xen:4.5.0:~::~~::
cpe:2.3:o:xen:xen:4.5.0:rc1:~::~~::
cpe:2.3:o:xen:xen:4.5.0:rc2:~::~~::
cpe:2.3:o:xen:xen:4.5.0:rc3:~::~~::

cpe:2.3:o:xen:xen:4.5.0:rc4:*****:
cpe:2.3:o:xen:xen:4.5.1:*****:
cpe:2.3:o:xen:xen:4.5.1:rc1:*****:
cpe:2.3:o:xen:xen:4.5.1:rc2:*****:
cpe:2.3:o:xen:xen:4.5.2:*****:
cpe:2.3:o:xen:xen:4.5.3:*****:
cpe:2.3:o:xen:xen:4.5.4:*****:
cpe:2.3:o:xen:xen:4.5.5:*****:
cpe:2.3:o:xen:xen:4.6.0:*****:
cpe:2.3:o:xen:xen:4.6.0:rc1:*****:
cpe:2.3:o:xen:xen:4.6.0:rc2:*****:
cpe:2.3:o:xen:xen:4.6.0:rc3:*****:
cpe:2.3:o:xen:xen:4.6.0:rc4:*****:
cpe:2.3:o:xen:xen:4.6.0:rc5:*****:
cpe:2.3:o:xen:xen:4.6.1:*****:
cpe:2.3:o:xen:xen:4.6.2:*****:
cpe:2.3:o:xen:xen:4.6.3:*****:
cpe:2.3:o:xen:xen:4.6.4:*****:
cpe:2.3:o:xen:xen:4.6.5:*****:
cpe:2.3:o:xen:xen:4.6.6:*****:
cpe:2.3:o:xen:xen:4.7.0:*****:
cpe:2.3:o:xen:xen:4.7.0:rc1:*****:
cpe:2.3:o:xen:xen:4.7.0:rc2:*****:
cpe:2.3:o:xen:xen:4.7.0:rc3:*****:
cpe:2.3:o:xen:xen:4.7.0:rc4:*****:
cpe:2.3:o:xen:xen:4.7.0:rc5:*****:
cpe:2.3:o:xen:xen:4.7.0:rc6:*****:
cpe:2.3:o:xen:xen:4.7.1:*****:
cpe:2.3:o:xen:xen:4.7.2:*****:

```
cpe:2.3:o:xen:xen:4.9.0:rc9:*:*:*:*:*:
```

© [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](#)