

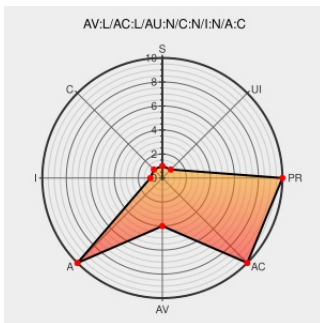


CVE-2015-7812

Published on: 11/17/2015 12:00:00 AM UTC

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

CVE-2015-7812

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

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

The hypercall_create_continuation function in arch/arm/domain.c in Xen 4.4.x through 4.6.x allows local guest users to cause a denial of service (host crash) via a preemptible hypercall to the multicall interface.

CVE-2015-7812 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

[SECURITY] Fedora 21 Update: xen-4.4.3-7.fc21

[lists.fedoraproject.org](#)
text/html

FEDORA FEDORA-2015-242be2c240

[SECURITY] Fedora 23 Update: xen-4.5.1-14.fc23

[lists.fedoraproject.org](#)
text/html

FEDORA FEDORA-2015-a931b02be2

Xen ARM Multicall Processing Bug Lets Local Users on a Guest System Cause Denial of Service Conditions on the Host System - SecurityTracker

[www.securitytracker.com](#)
text/html

SECTRAK 1034031

Debian -- Security Information -- DSA-3414-1 xen

[www.debian.org](#)
Deprecated Link
text/html

DEBIAN DSA-3414

XSA-145 - Xen Security Advisories

Patch
Vendor Advisory
[xenbits.xen.org](#)
text/html

CONFIRM
[xenbits.xen.org/xsa/advisory-145.html](#)

Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security

[security.gentoo.org](https://security.gentoo.org/text/html)
text/html

 GENTOO GLSA-201604-03

[SECURITY] Fedora 22 Update: xen-4.5.1-14.fc22

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
text/html

 FEDORA FEDORA-2015-6f6b79efe2

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	4.4.1	-	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	4.5.0	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	4.6.0	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.1	-	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	4.5.0	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	4.6.0	All	All	All

System

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:

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:4.5.0:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.2:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:

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:4.5.0:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.2:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:

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](#)