

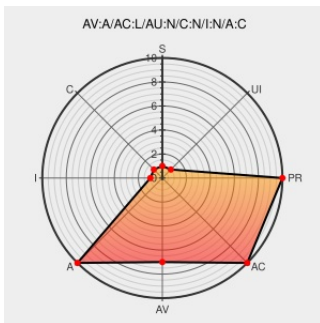


CVE-2014-7154

Published on: 10/02/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:48 PM UTC

CVE-2014-7154

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

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

Race condition in HVMOP_track_dirty_vram in Xen 4.0.0 through 4.4.x does not ensure possession of the guarding lock for dirty video RAM tracking, which allows certain local guest domains to cause a denial of service via unspecified vectors.

CVE-2014-7154 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.1 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

[SECURITY] Fedora 20 Update: xen-4.3.3-3.fc20

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

[FEDORA FEDORA-2014-12036](#)

XSA-104 - Xen Security Advisories

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

[CONFIRM](#)
[xenbits.xen.org/xsa/advisory-104.html](#)

[security-announce] openSUSE-SU-2014:1279-1: important: xen: security an

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

[SUSE openSUSE-SU-2014:1279](#)

Xen HVMOP_track_dirty_vram Race Condition Lets Local Guest Users Deny Service on the Host System - SecurityTracker

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

[SECTrack 1030887](#)

text/html

Debian -- Security Information -- DSA-3041-1 xen

Third Party Advisory

www.debian.org

Deprecated Link

text/html

 DEBIAN DSA-3041

Security Advisory SA61890 - Gentoo update for xen - Secunia

web.archive.org

text/html

 SECUNIA 61890

Xen: Denial of Service (GLSA 201412-42) — Gentoo security

security.gentoo.org

text/html

 GENTOO GLSA-201412-42

[SECURITY] Fedora 19 Update: xen-4.2.5-3.fc19

Third Party Advisory

lists.fedoraproject.org

text/html

 FEDORA FEDORA-2014-12000

Security Advisory SA61501 - Xen "shadow_track_dirty_vram()" Race Condition Denial of Service Vulnerability - Secunia

web.archive.org

text/html

 SECUNIA 61501

[security-announce] openSUSE-SU-2014:1281-1: important: xen: security an

Third Party Advisory

lists.opensuse.org

text/html

 SUSE openSUSE-SU-2014:1281

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	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All

Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	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
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
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6.1	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
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
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:fedoraproject:fedora:19:*****:						
cpe:2.3:o:fedoraproject:fedora:20:*****:						
cpe:2.3:o:fedoraproject:fedora:19:*****:						
cpe:2.3:o:fedoraproject:fedora:20:*****:						
cpe:2.3:o:opensuse:opensuse:12.3:*****:						
cpe:2.3:o:opensuse:opensuse:13.1:*****:						
cpe:2.3:o:opensuse:opensuse:12.3:*****:						
cpe:2.3:o:opensuse:opensuse:13.1:*****:						
cpe:2.3:o:xen:xen:4.1.0:*****:						
cpe:2.3:o:xen:xen:4.1.1:*****:						
cpe:2.3:o:xen:xen:4.1.2:*****:						
cpe:2.3:o:xen:xen:4.1.3:*****:						
cpe:2.3:o:xen:xen:4.1.4:*****:						
cpe:2.3:o:xen:xen:4.1.5:*****:						
cpe:2.3:o:xen:xen:4.1.6.1:*****:						

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:*****:
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:4.1.0:*****:
cpe:2.3:o:xen:xen:4.1.1:*****:
cpe:2.3:o:xen:xen:4.1.2:*****:
cpe:2.3:o:xen:xen:4.1.3:*****:
cpe:2.3:o:xen:xen:4.1.4:*****:
cpe:2.3:o:xen:xen:4.1.5:*****:
cpe:2.3:o:xen:xen:4.1.6.1:*****:
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:*****:
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:-:*****:

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](#)