



CVE-2013-1442

Published on: 09/30/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:32 PM UTC

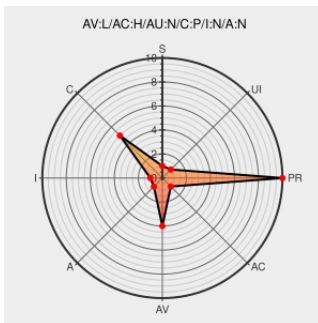
CVE-2013-1442

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Xen 4.0 through 4.3.x, when using AVX or LWP capable CPUs, does not properly clear previous data from registers when using an XSAVE or XRSTOR to extend the state components of a saved or restored vCPU after touching other restored extended registers, which allows local guest OSes to obtain sensitive information by reading the registers.

CVE-2013-1442 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: **1.2 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3006-1 xen	www.debian.org Deprecated Link text/html	DEBIAN DSA-3006
Xen AVX/LWP XSAVE/XRSTOR May Disclose Sensitive Information to Local Users - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1029090
openSUSE-SU-2013:1636-1: moderate: xen: security and bugfix update to 4.	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1636
oss-security - Xen Security Advisory 62 (CVE-2013-1442) - Information leak on AVX and/or LWP capable CPUs	www.openwall.com text/html	MLIST [oss-security] 20130925 Xen Security Advisory 62 (CVE-2013-1442) - Information leak on AVX and/or LWP capable CPUs
Gentoo Linux Documentation -- Xen: Multiple	security.gentoo.org	GENTOO GLSA-201407-03

Vunlerabilities

[security-announce] SUSE-SU-2014:0446-1: important: Security update for

lists.opensuse.org

text/html

 SUSE SUSE-SU-2014:0446

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	4.0.0	All	All	All
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	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	4.2.0	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	Xen	Xen	4.0.0	All	All	All

System						
Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	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	4.2.0	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
cpe:2.3:o:xen:xen:4.0.0:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.0.1:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.0.2:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.0.3:*:*:*:*:*:						
cpe:2.3:o:xen:xen:4.0.4:*:*:*:*:*:						
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:4.2.0:*****:
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:4.0.0:*****:
cpe:2.3:o:xen:xen:4.0.1:*****:
cpe:2.3:o:xen:xen:4.0.2:*****:
cpe:2.3:o:xen:xen:4.0.3:*****:
cpe:2.3:o:xen:xen:4.0.4:*****:
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:4.2.0:*****:
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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)