

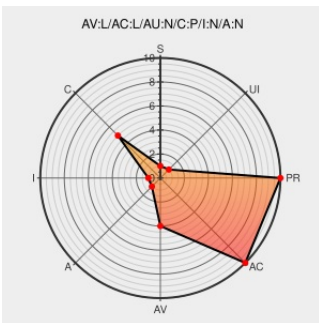


CVE-2013-4361

Published on: 10/01/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:13 AM UTC

CVE-2013-4361

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

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

The fbld instruction emulation in Xen 3.3.x through 4.3.x does not use the correct variable for the source effective address, which allows local HVM guests to obtain hypervisor stack information by reading the values used by the instruction.

CVE-2013-4361 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Debian -- Security Information -- DSA-3006-1 xen

www.debian.org

Deprecated Link

text/html

[DEBIAN DSA-3006](#)

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 66 (CVE-2013-4361) - Information leak through fbld instruction emulation

www.openwall.com

text/html

[MLIST \[oss-security\] 20130930 Xen Security Advisory 66 \(CVE-2013-4361\) - Information leak through fbld instruction emulation](#)

Gentoo Linux Documentation -- Xen: Multiple Vulnerabilities

security.gentoo.org

text/html

[GENTOO GLSA-201407-03](#)

[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	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
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	4.3.0	All	All	All
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
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	4.3.0	All	All	All
cpe:2.3:o:xen:xen:3.3.0:*****:						
cpe:2.3:o:xen:xen:3.3.1:*****:						
cpe:2.3:o:xen:xen:3.3.2:*****:						
cpe:2.3:o:xen:xen:3.4.0:*****:						
cpe:2.3:o:xen:xen:3.4.1:*****:						
cpe:2.3:o:xen:xen:3.4.2:*****:						
cpe:2.3:o:xen:xen:3.4.3:*****:						
cpe:2.3:o:xen:xen:3.4.4:*****:						
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:4.3.0:*****:
cpe:2.3:o:xen:xen:3.3.0:*****:
cpe:2.3:o:xen:xen:3.3.1:*****:
cpe:2.3:o:xen:xen:3.3.2:*****:
cpe:2.3:o:xen:xen:3.4.0:*****:
cpe:2.3:o:xen:xen:3.4.1:*****:
cpe:2.3:o:xen:xen:3.4.2:*****:
cpe:2.3:o:xen:xen:3.4.3:*****:
cpe:2.3:o:xen:xen:3.4.4:*****:
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:4.3.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)