

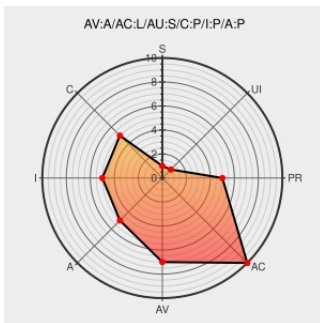


CVE-2013-4554

Published on: 12/24/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:24 AM UTC

CVE-2013-4554

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

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

Xen 3.0.3 through 4.1.x (possibly 4.1.6.1), 4.2.x (possibly 4.2.3), and 4.3.x (possibly 4.3.1) does not properly prevent access to hypercalls, which allows local guest users to gain privileges via a crafted application running in ring 1 or 2.

CVE-2013-4554 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.2 - MEDIUM**

Access
Vector

ADJACENT_NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

oss-security - Xen Security Advisory 76 (CVE-2013-4554) - Hypercalls exposed to privilege rings 1 and 2 of HVM guests

www.openwall.com
text/html

[MLIST \[oss-security\] 20131126 Xen Security Advisory 76 \(CVE-2013-4554\) - Hypercalls exposed to privilege rings 1 and 2 of HVM guests](#)

[security-announce] SUSE-SU-2014:0411-1: important: Security update for

lists.opensuse.org
text/html

[SUSE SUSE-SU-2014:0411](#)

Red Hat Customer Portal

web.archive.org
text/html
Inactive Link **Not Archived**

[REDHAT RHSA-2014:0285](#)

openSUSE-SU-2013:1876-1: moderate: xen: security and bugfix update

lists.opensuse.org
text/html

[SUSE openSUSE-SU-2013:1876](#)

Gentoo Linux Documentation -- Xen: Multiple Vulnerabilities

security.gentoo.org
text/html

[GENTOO GLSA-201407-03](#)

[security-announce] SUSE-SU-2014:0470-1: important:
Security update for

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

 SUSE SUSE-SU-2014:0470

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

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

 SUSE SUSE-SU-2014:0446

[security-announce] SUSE-SU-2014:0372-1: important:
Security update for

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

 SUSE SUSE-SU-2014:0372

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	3.0.3	All	All	All
Operating System	Xen	Xen	3.0.4	All	All	All
Operating System	Xen	Xen	3.1.3	All	All	All
Operating System	Xen	Xen	3.1.4	All	All	All
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	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	4.1.6.1	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	3.0.3	All	All	All
Operating System	Xen	Xen	3.0.4	All	All	All
Operating System	Xen	Xen	3.1.3	All	All	All
Operating System	Xen	Xen	3.1.4	All	All	All

Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	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	4.1.6.1	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
cpe:2.3:o:xen:xen:3.0.3:*****:						
cpe:2.3:o:xen:xen:3.0.4:*****:						
cpe:2.3:o:xen:xen:3.1.3:*****:						
cpe:2.3:o:xen:xen:3.1.4:*****:						
cpe:2.3:o:xen:xen:3.2.0:*****:						
cpe:2.3:o:xen:xen:3.2.1:*****:						
cpe:2.3:o:xen:xen:3.2.2:*****:						
cpe:2.3:o:xen:xen:3.2.3:*****:						
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:4.0.4:*****:
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:4.1.6.1:*****:
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:3.0.3:*****:
cpe:2.3:o:xen:xen:3.0.4:*****:
cpe:2.3:o:xen:xen:3.1.3:*****:
cpe:2.3:o:xen:xen:3.1.4:*****:
cpe:2.3:o:xen:xen:3.2.0:*****:
cpe:2.3:o:xen:xen:3.2.1:*****:
cpe:2.3:o:xen:xen:3.2.2:*****:
cpe:2.3:o:xen:xen:3.2.3:*****:
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:4.1.6.1:*****:
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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)