

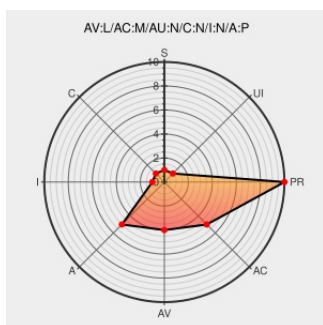


CVE-2013-1917

Published on: 05/13/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:14 AM UTC

CVE-2013-1917

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

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

Xen 3.1 through 4.x, when running 64-bit hosts on Intel CPUs, does not clear the NT flag when using an IRET after a SYSENTER instruction, which allows PV guest users to cause a denial of service (hypervisor crash) by triggering a #GP fault, which is not properly handled by another IRET instruction.

CVE-2013-1917 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **1.9 - LOW**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

oss-security - Xen Security Advisory 44 (CVE-2013-1917) - Xen PV DoS vulnerability with SYSENTER

www.openwall.com
text/html

MLIST [oss-security] 20130418 Xen Security Advisory 44 (CVE-2013-1917) - Xen PV DoS vulnerability with SYSENTER

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

lists.opensuse.org
text/html

SUSE SUSE-SU-2014:0411

Xen SYSENTER Processing Error Lets Local PV Guest Users Deny Service on the Host System - SecurityTracker

www.securitytracker.com
text/html

SECTrack 1028455

Debian -- Page not found

www.debian.org
Deprecated Link
text/html
Inactive Link Not Archived

DEBIAN DSA-2662

Security Advisory SA55082 - Gentoo update for xen - Secunia

web.archive.org
text/html

SECUNIA 55082

[SECURITY] Fedora 17 Update: xen-4.1.5-1.fc17	lists.fedoraproject.org text/html	 FEDORA FEDORA-2013-6723
[security-announce] SUSE-SU-2014:0470-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2014:0470
Gentoo Linux Documentation -- Xen: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-201309-24
[security-announce] SUSE-SU-2014:0446-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2014:0446
openSUSE-SU-2013:0912-1: moderate: xen up to xsa-47	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0912

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	3.1.3	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

System						
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	4.2.0	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	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

System						
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	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
	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:4.2.0:*****:
cpe:2.3:o:xen:xen:4.2.1:*****:
cpe:2.3:o:xen:xen:4.2.2:*****:
cpe:2.3:o:xen:xen: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:4.2.0:*****:
cpe:2.3:o:xen:xen:4.2.1:*****:
cpe:2.3:o:xen:xen:4.2.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)