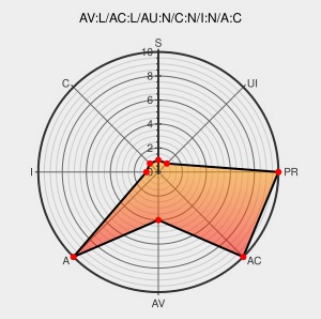
CVE-2015-5307

Published on: 11/16/2015 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:15:00 PM UTC

CVE-2015-5307

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #AC (aka Alignment Check) exceptions, related to svm.c and vmx.c.

CVE-2015-5307 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
USN-2800-1: Linux kernel vulnerability | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-2800-1
Red Hat Customer Portal	access.redhat.com, text/html	MISC access.redhat.com/errata/RHSA-2015:2552
[security-announce] SUSE-SU-2015:2350-1: important: Security update for	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SU-2015:2350
USN-2805-1: Linux kernel (Utopic HWE) vulnerability | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-2805-1
Citrix XenServer Security	Third Party Advisory	CONFIRM support.citrix.com/article/CTX202583

Update for CVE-2015-5307 and CVE-2015-8104	support.citrix.com text/html	
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0046
[security-announce] SUSE-SU-2016:0354-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:0354
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0004
KVM: x86: work around infinite loop in microcode when #AC is delivered · torvalds/linux@54a2055 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/54a20552e1eae07aa240fa370a0293e006b5faed
Debian -- Security Information -- DSA-3454-1 virtualbox	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3454
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2636
Debian -- Security Information -- DSA-3396-1 linux	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3396
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2587
USN-2804-1: Linux kernel (Trusty HWE) vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2804-1
2017-04 Security Bulletin: Multiple Vulnerabilities in NorthStar Controller Application before version 2.1.0 Service Pack 1. - Juniper Networks	Third Party Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA10783
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2636
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2645
USN-2801-1: Linux kernel vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2801-1
XSA-156 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-156.html

Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0024
CVE-2015-5307 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-5307
Oracle VM Server for x86 Bulletin - July 2016	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
[security-announce] SUSE-SU-2015:2108-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2015:2108
openSUSE-SU-2015:2250-1: moderate: Security update for xen	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2250
[security-announce] SUSE-SU-2016:2074-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2016:2074
[security-announce] SUSE-SU-2015:2194-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2015:2194
[security-announce] SUSE-SU-2015:2339-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2015:2339
Debian -- Security Information -- DSA-3414-1 xen	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3414
Bug 1277172 – CVE-2015-5307 virt: guest to host DoS by triggering an infinite loop in microcode via #AC exception	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1277172
Oracle Linux Bulletin - October 2015	Vendor Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
[SECURITY] Fedora 22 Update: xen-4.5.2-2.fc22	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2015-668d213dc3
USN-2802-1: Linux kernel vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2802-1
USN-2807-1: Linux kernel (Wily HWE) vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2807-1
[SECURITY] Fedora 23 Update: xen-4.5.2-2.fc23	Mailing List Third Party Advisory lists.fedoraproject.org	FEDORA FEDORA-2015-394835a3f6

	text/html	
Oracle Linux Bulletin - January 2016	Vendor Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=54a20552e1eae07aa240fa370a0293e006b5faed
[SECURITY] Fedora 21 Update: xen-4.4.3-8.fc21	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2015-f150b2a8c8
Linux Kernel CVE-2015-5307 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 77528
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:0046
openSUSE-SU-2015:2232-1: moderate: Security update for the Linux Kernel	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2232
Xen Exception Handling Bugs Let Local Users on a Guest System Cause Denial of Service Conditions on the Host System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1034105
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2015:2645
USN-2806-1: Linux kernel (Vivid HWE) vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2806-1
oss-security - Re: CVE-2015-5307 kernel: kvm: guest to host DoS by triggering an infinite loop in microcode via #AC exception	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20151110 Re: CVE-2015-5307 kernel: kvm: guest to host DoS by triggering an infinite loop in microcode via #AC exception
USN-2803-1: Linux kernel vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-2803-1
Oracle Critical Patch Update - January 2016	Patch Vendor Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	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	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.1	All	All	All

Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.4.4	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.2	All	All	All
Operating System	Xen	Xen	4.5.3	All	All	All
Operating System	Xen	Xen	4.5.5	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.6.2	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.6.4	All	All	All
Operating System	Xen	Xen	4.6.5	All	All	All
Operating System	Xen	Xen	4.6.6	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	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.1	All	All	All
Operating System	Xen	Xen	4.4.2	All	All	All

Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.4.4	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.2	All	All	All
Operating System	Xen	Xen	4.5.3	All	All	All
Operating System	Xen	Xen	4.5.5	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.6.2	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.6.4	All	All	All
Operating System	Xen	Xen	4.6.5	All	All	All
Operating System	Xen	Xen	4.6.6	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_virtualbox:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_virtualbox:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_virtualbox:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_virtualbox:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:vm_virtualbox:*:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.6:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.5:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.4:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.5:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.6:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report