

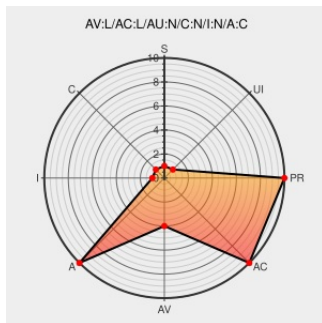


CVE-2009-2287

Published on: 07/01/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:30 PM UTC

CVE-2009-2287

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The `kvm_arch_vcpu_ioctl_set_sregs` function in the KVM in Linux kernel 2.6 before 2.6.30, when running on x86 systems, does not validate the page table root in a `KVM_SET_SREGS` call, which allows local users to cause a denial of service (crash or hang) via a crafted `cr3` value, which triggers a NULL pointer dereference in the

`gfn_to_rmap` function.

CVE-2009-2287 has been assigned by [M](#) `cve@mitre.org` to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

SourceForge.net: kernel virtual machine: Detail: 2687641 - EXPLOITABLE failure to validate cr3 after KVM_SET_SREGS

[Third Party Advisory](#)
[sourceforge.net](#)
[text/html](#)

[CONFIRM](#) sourceforge.net/tracker/?func=detail&atid=893831&aid=2687641&g

USN-807-1: Linux kernel vulnerabilities | Ubuntu

[Third Party Advisory](#)
[www.ubuntu.com](#)
[text/html](#)

[UBUNTU](#) [USN-807-1](#)

kernel/git/torvalds/linux.git - Linux kernel source tree

[Mailing List](#)
[Patch](#)
[Vendor Advisory](#)
[git.kernel.org](#)
[text/html](#)

[CONFIRM](#) git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=59839dfff5eabca01cc4e20b45797a60a80af8cb

Support / Security / Advisories / / MDVSA-2010:198 Mandriva	text/html Broken Link www.mandriva.com text/html	 MANDRIVA MDVSA-2010:198
Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	Broken Link web.archive.org text/html	 SECUNIA 36045
KVM "kvm_arch_vcpu_ioctl_set_sregs()" Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com	Broken Link web.archive.org text/html	 SECUNIA 35675
Debian -- Security Information -- DSA-1845-1 linux-2.6	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-1845
oss-security - CVE Request: kernel: kvm: failure to validate cr3 after KVM_SET_SREGS	Mailing List Patch Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20090630 CVE Request: kernel: kvm: failure to validate c
Debian update for linux-2.6 - Secunia Advisories - Vulnerability Information - Secunia.com	Broken Link web.archive.org text/html	 SECUNIA 36054
kvm-x86-check-for-cr3-validity-in-ioctl_set_sregs.patch « queue-2.6.30 - kernel/git/stable/stable-queue.git - Linux kernel stable patch queue	Mailing List Patch Vendor Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/?p=linux/kernel/git/stable/stable-queue.git;a=blob;f=queue-2.6.30-kvm-x86-check-for-cr3-validity-in-ioctl_set_sregs.patch;h=b48a47dad2cf76358b327368f80c0805e6370c68;hb=e7c4

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	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All

Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:6.06:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:8.04:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:8.10:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:9.04:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:6.06:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:8.04:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:8.10:~::~::~:						
cpe:2.3:o:canonical:ubuntu_linux:9.04:~::~::~:						
cpe:2.3:o:debian:debian_linux:4.0:~::~::~:						
cpe:2.3:o:debian:debian_linux:5.0:~::~::~:						
cpe:2.3:o:debian:debian_linux:4.0:~::~::~:						
cpe:2.3:o:debian:debian_linux:5.0:~::~::~:						
cpe:2.3:o:linux:linux_kernel:~::~::~:						
cpe:2.3:o:linux:linux_kernel:~::~::~:						

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](#)