



CVE-2009-3638

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-3638
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-29 14:30:00 UTC
Updated	2023-02-13 02:20:00 UTC
Description	Integer overflow in the kvm_dev_ioctl_get_supported_cpuid function in arch/x86/kvm/x86.c in the KVM subsystem in the Lin

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Operating System	Linux	Linux Kernel	2.6.23.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.23.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.25	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.19	All	All	All

[illegible]

[illegible]

Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References						
Reference				Source	Link	
[SECURITY] Fedora 10 Update: kernel-2.6.27.38-170.2.113.fc10				FEDORA	www.redhat.com	
kernel/git/torvalds/linux.git - Linux kernel source tree				CONFIRM	git.kernel.org	
404: File not found				CONFIRM	www.kernel.org	
Linux Kernel KVM 'kvm_dev_ioctl_get_supported_cpuid()' Integer Overflow Vulnerability				BID	www.securityfocus.com	
USN-864-1: Linux kernel vulnerabilities Ubuntu				UBUNTU	www.ubuntu.com	
Support / Security / Advisories / / MDVSA-2009:329 Mandriva				MANDRIVA	www.mandriva.com	
kernel/git/torvalds/linux.git - Linux kernel source tree				MISC	git.kernel.org	
404: File not found				CONFIRM	www.kernel.org	
CVE-2009-3638 - Red Hat Customer Portal				MISC	access.redhat.com	
IBM X-Force Exchange				XF	exchange.xforce.ibmcloud.com	
'Re: [oss-security] CVE request: kvm: integer overflow in' - MARC				MLIST	marc.info	
Bug 530515 – CVE-2009-3638 kernel: kvm: integer overflow in kvm_dev_ioctl_get_supported_cpuid()				CONFIRM	bugzilla.redhat.com	
'[oss-security] CVE request: kvm: integer overflow in kvm_dev_ioctl_get_supported_cpuid()' - MARC				MLIST	marc.info	

CVE-2009-3638 - Red Hat Customer Portal	CVE-2009-3638 - Red Hat Customer Portal
---	---

CVE Program record

CVE.ORG

www.cve.org

NVD vulnerability detail

NVD

nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-10-30	Tomas Hoger	Not vulnerable. This issue did not affect the versions of KVM as shipped with Red Hat Enterprise Linux 5.5 and 5.6.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API cve.report/api

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