



CVE-2009-4004

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

Summary

CVE	CVE-2009-4004
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-11-20 02:30:00 UTC
Updated	2023-11-07 02:04:00 UTC
Description	Buffer overflow in the kvm_vcpu_ioctl_x86_setup_mce function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.32	-	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.32	-	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.32	rc6	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
Linux Kernel Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
git.kernel.org		git.kernel.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.c
Linux Kernel KVM 'KVM_MAX_MCE_BANKS' Memory Corruption Vulnerability	BID	www.securityfocus.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
404: File not found	CONFIRM	www.kernel.org
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	2009-11-20	Tomas Hoger	Not vulnerable. This issue did not affect the versions of Linux kernel as shipped with Red Hat E

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