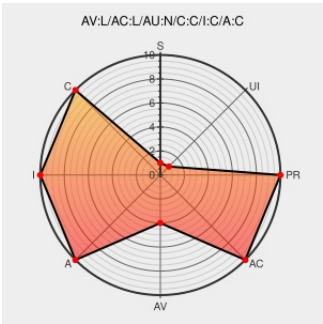
CVE-2009-3290

Published on: 09/22/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:24 PM UTC

CVE-2009-3290

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The kvm_emulate_hypercall function in arch/x86/kvm/x86.c in KVM in the Linux kernel 2.6.25-rc1, and other versions before 2.6.31, when running on x86 systems, does not prevent access to MMU hypercalls from ring 0, which allows local guest OS users to cause a denial of service (guest kernel crash) and read or write guest kernel memory via unspecified "random addresses."

CVE-2009-3290 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
[v2] KVM: x86: Disallow hypercalls for guest callers in rings > 0 - Patchwork	Patch, patchwork.kernel.org, text/html	CONFIRM patchwork.kernel.org/patch/38926/
Bug 524124 – CVE-2009-3290 kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0	bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=524124
oss-security - Re: CVE request: kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0	www.openwall.com, text/html	MLIST [oss-security] 20090921 Re: CVE request: kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org, text/html	CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=07708c4af1346ab1521b26a202f438366b7bcffd

Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 37105
Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2009:1465
oss-security - Re: CVE request: kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0	www.openwall.com text/html	MLIST [oss-security] 20090922 Re: CVE request: kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0
oss-security - CVE request: kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0	www.openwall.com text/html	MLIST [oss-security] 20090918 CVE request: kernel: KVM: x86: Disallow hypercalls for guest callers in rings > 0
USN-852-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-852-1
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11328

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.25	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.25	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.25:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.25:rc1:*:*:*:*:*:*:

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

← Previous ID

Next ID→

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