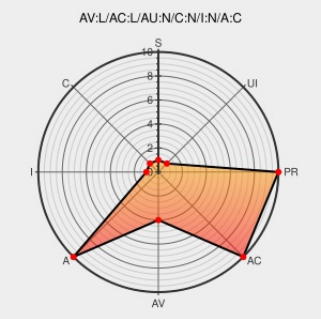
CVE-2012-1601

Published on: 05/17/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:13 AM UTC

CVE-2012-1601

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



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

The KVM implementation in the Linux kernel before 3.3.6 allows host OS users to cause a denial of service (NULL pointer dereference and host OS crash) by making a KVM_CREATE_IRQCHIP ioctl call after a virtual CPU already exists.

CVE-2012-1601 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
oss-security - Re: CVE request -- kernel: kvm: irqchip_in_kernel() and vcpu->arch.apic inconsistency	www.openwall.com text/html	MLIST [oss-security] 20120329 Re: CVE request -- kernel: kvm: irqchip_in_kernel() and vcpu->arch.apic inconsistency
Security Advisory SA49928 - Ubuntu update for linux - Secunia	web.archive.org text/html	SECUNIA 49928
[security-announce] openSUSE-SU-2013:0925-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0925
KVM Null Pointer Dereference in	www.securitytracker.com text/html	SECTRACK 1026897

irqchip_in_kernel() Lets Local Users Deny Service - SecurityTracker		
KVM: Ensure all vcpus are consistent with in-kernel irqchip settings · torvalds/linux@9c89516 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/9c895160d25a76c21b65bad141b08e8d4f99afef
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.3.6
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2012:0676
Debian -- Security Information -- DSA-2469-1 linux-2.6	www.debian.org Depreciated Link text/html	DEBIAN DSA-2469
808199 – (CVE-2012-1601) CVE-2012-1601 kernel: kvm: irqchip_in_kernel() and vcpu->arch.apic inconsistency	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=808199
SUSE-SU-2012:1679-1	www.suse.com text/html	SUSE SUSE-SU-2012:1679
No Description Provided	rhn.redhat.com Inactive Link Not Archived	REDHAT RHSA-2012:0571

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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