

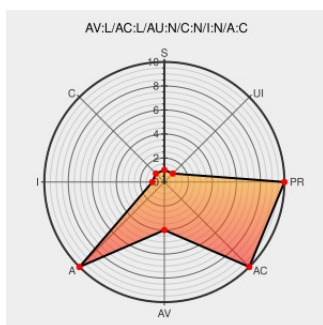


CVE-2012-1601

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

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

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	text/html	
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 Deprecated 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

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	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 →](#)

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](#)