

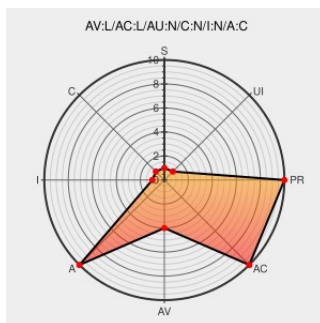


CVE-2012-2121

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

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2012-2121

[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 3.3.4 does not properly manage the relationships between memory slots and the iommu, which allows guest OS users to cause a denial of service (memory leak and host OS crash) by leveraging administrative access to the guest OS to conduct hotunplug and hotplug operations on

devices.

CVE-2012-2121 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: device assignment page leak

www.openwall.com
text/html

[MLIST \[oss-security\] 20120419 Re: CVE request -- kernel: kvm: device assignment page leak](#)

USN-2037-1: Linux kernel (EC2) vulnerabilities | Ubuntu

www.ubuntu.com
text/html

[UBUNTU USN-2037-1](#)

Bug 814149 – CVE-2012-2121 kvm: device assignment page leak

bugzilla.redhat.com
text/html

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=814149](http://bugzilla.redhat.com/show_bug.cgi?id=814149)

USN-2036-1: Linux kernel

www.ubuntu.com

[UBUNTU USN-2036-1](#)

CONFIRM Ubuntu Kernel vulnerabilities | Ubuntu

[www.ubuntu.com](#)
text/html

UBUNTU CONFIRM

Red Hat Customer Portal

[web.archive.org](#)
text/html
Inactive Link Not Archived

REDHAT RHSA-2012:0676

Security Alerts - Secunia

[web.archive.org](#)
text/html

SECUNIA 50732

Red Hat Customer Portal

[web.archive.org](#)
text/html
Inactive Link Not Archived

REDHAT RHSA-2012:0743

[www.kernel.org](#)
text/plain

CONFIRM [www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.3.4](#)

Linux Kernel KVM Memory Slot Management Flaw Lets Local Guest Users Deny Service on the Guest Operating System - SecurityTracker

[www.securitytracker.com](#)
text/html

SECTrack 1027083

KVM: unmap pages from the iommu when slots are removed · torvalds/linux@09ca8e1 · GitHub

[github.com](#)
text/html

CONFIRM [github.com/torvalds/linux/commit/09ca8e1173bcb12e2a449698c9ae3b86a8a10195](#)

USN-1577-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu

[www.ubuntu.com](#)
text/html

UBUNTU USN-1577-1

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

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](#)