



CVE-2016-5412

Published on: 08/06/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:24:00 PM UTC

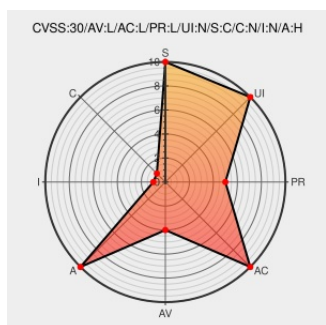
CVE-2016-5412

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

arch/powerpc/kvm/book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when CONFIG_KVM_BOOK3S_64_HV is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDC hypercall during the existence of a suspended transaction.

CVE-2016-5412 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

LOCAL

LOW

LOW

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

CHANGED

NONE

NONE

HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector

Access Complexity

Authentication

LOCAL

LOW

SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Red Hat Customer Portal

[access.redhat.com](https://access.redhat.com/text/html)
text/html

MISC access.redhat.com/errata/RHSA-2016:2574

linux-security - CVE-2016-

[Mailing List](#)

MISC [linux-security/20160728/CVE-2016-5412_Kernel_powerpc_kvm_Infinite](#)

CVE 2016-5412 Kernel: powerpc: kvm: Infinite loop via H_CEDE hypercall when running under hypervisor-mode

mailing list

www.openwall.com

text/html

kernel/git/torvalds/linux.git - Linux kernel source tree

git.kernel.org

text/html

CONFIRM

git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=93d17397e4e2182fdaad503e2f9da46202c0f1c3

kernel/git/torvalds/linux.git - Linux kernel source tree

git.kernel.org

text/html

CONFIRM

git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=f024ee098476a3e620232e4a78cfac505f121245

Red Hat Customer Portal

web.archive.org

text/html

Inactive Link

Not Archived

REDHAT

RHSA-2016:2574

Bug 1349916 – CVE-2016-5412 Kernel: powerpc: kvm: Infinite loop via H_CEDE hypercall when running under hypervisor-mode

Issue Tracking

Patch

Third Party Advisory

bugzilla.redhat.com

text/html

CONFIRM

bugzilla.redhat.com/show_bug.cgi?id=1349916

KVM: PPC: Book3S HV: Pull out TM state save/restore into separate pro... · torvalds/linux@f024ee0 · GitHub

github.com

text/html

CONFIRM

github.com/torvalds/linux/commit/f024ee098476a3e620232e4a78cfac505f121245

CVE-2016-5412 - Red Hat Customer Portal

access.redhat.com

text/html

MISC

access.redhat.com/security/cve/CVE-2016-5412

KVM: PPC: Book3S HV: Save/restore TM state in H_CEDE · torvalds/linux@93d1739 · GitHub

github.com

text/html

CONFIRM

github.com/torvalds/linux/commit/93d17397e4e2182fdaad503e2f9da46202c0f1c3

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 →

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)