



CVE-2012-1179

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

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

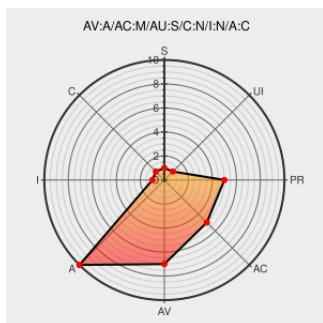
CVE-2012-1179

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The Linux kernel before 3.3.1, when KVM is used, allows guest OS users to cause a denial of service (host OS crash) by leveraging administrative access to the guest OS, related to the `pmd_none_or_clear_bad` function and page faults for huge pages.

CVE-2012-1179 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.2 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

MEDIUM

SINGLE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

oss-security - CVE-2012-1179 kernel: thp: `__split_huge_page()` `mapcount != page_mapcount` `BUG_ON()`

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

MLIST [oss-security] 20120315 CVE-2012-1179 kernel: thp: `__split_huge_page()` `mapcount != page_mapcount` `BUG_ON()`

[security-announce]
SUSE-SU-2012:0554-1:
important: Security update
for

lists.opensuse.org
[text/html](#)

SUSE SUSE-SU-2012:0554

Security Advisory
SA48404 - Linux Kernel
"`__split_huge_page()`"
Race Condition Denial of
Service Vulnerability

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

SECUNIA 48404

Service vulnerability - Secunia

Linux Kernel KVM pmd_none_or_clear_bad() Bug Lets Local Guest Users Cause Denial of Service Conditions on the Host System - SecurityTracker	www.kernel.org text/plain	 CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.3.1
Bug 803793 – CVE-2012-1179 kernel: thp: __split_huge_page() mapcount != page_mapcount BUG_ON()	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=803793
mm: thp: fix pmd_bad() triggering in code paths holding mmap_sem read... · torvalds/linux@4a1d704 · GitHub	github.com text/html	 CONFIRM github.com/torvalds/linux/commit/4a1d704194a441bf83c636004a479e01360ec850
'[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC	marc.info text/html	 HP HPSBGN02970
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0743
[SECURITY] Fedora 16 Update: kernel-3.2.10- 3.fc16	lists.fedoraproject.org text/html	 FEDORA FEDORA-2012-3712
Security Advisory SA48898 - SUSE update for kernel - Secunia	web.archive.org text/html	 SECUNIA 48898

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	rc7	All	All
cpe:2.3:o:linux:linux_kernel:*:rc7:*:*:*:*:						

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](#)