



CVE-2015-4177

Published on: 05/02/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:03 PM UTC

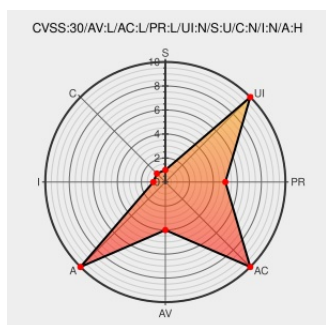
CVE-2015-4177

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The collect_mounts function in fs/namespace.c in the Linux kernel before 4.0.5 does not properly consider that it may execute after a path has been unmounted, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call.

CVE-2015-4177 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

LOCAL

LOW

LOW

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

NONE

NONE

HIGH

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

Bug 1248486 – CVE-2015-4177
kernel: Race conditions in
collect_mounts

bugzilla.redhat.com
[text/html](#)

CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1248486

mnt: Fail collect_mounts when applied to unmounted mounts · torvalds/linux@cd4a401 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/cd4a40174b71acd021877341684d8bb1dc8ea4ae
oss-security - Re: CVE request Linux kernel: ns: user namespaces panic	www.openwall.com text/html	MLIST [oss-security] 20150604 Re: CVE request Linux kernel: ns: user namespaces panic
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.0.5
oss-security - CVE request Linux kernel: ns: user namespaces panic	openwall.com text/html	MLIST [oss-security] 20150529 CVE request Linux kernel: ns: user namespaces panic
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=cd4a40174b71acd021877341684d8bb1dc8ea4ae
oss-security - Re: CVE request Linux kernel: ns: user namespaces panic	openwall.com text/html	MLIST [oss-security] 20150529 Re: CVE request Linux kernel: ns: user namespaces panic

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 →](#)