

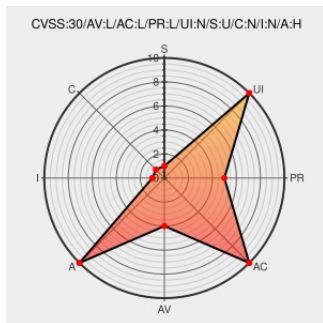


CVE-2015-4178

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

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

CVE-2015-4178

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The fs_pin implementation in the Linux kernel before 4.0.5 does not ensure the internal consistency of a certain list data structure, 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, related to fs/fs_pin.c and include/linux/fs_pin.h.

CVE-2015-4178 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
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=820f9f147dcce2602eefd9b575bbbd9ea14f0953
Bug 1249849 - CVE-2015-4178	bugzilla.redhat.com	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1249849

bug 1240040 - CVE 2010-4170 kernel: list corruption of m_list or s_list if unused	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1240040
oss-security - Re: Re: CVE request Linux kernel: ns: user namespaces panic	www.openwall.com text/html	MLIST [oss-security] 20150604 Re: Re: CVE request Linux kernel: ns: user namespaces panic
	Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.0.5
fs_pin: Allow for the possibility that m_list or s_list go unused. · torvalds/linux@820f9f1 · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/820f9f147dcce2602eefd9b575bbbd9ea14f0953
oss-security - CVE request Linux kernel: ns: user namespaces panic	Patch openwall.com text/html	MLIST [oss-security] 20150529 CVE request Linux kernel: ns: user namespaces panic
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