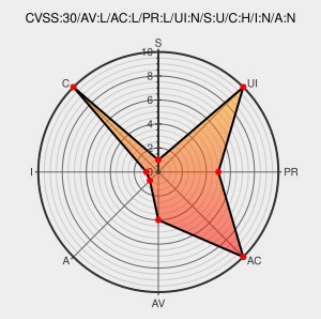
CVE-2015-4176

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

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

CVE-2015-4176

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

fs/namespace.c in the Linux kernel before 4.0.2 does not properly support mount connectivity, which allows local users to read arbitrary files by leveraging user-namespace root access for deletion of a file or directory.

CVE-2015-4176 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	HIGH	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
1249442 – (CVE-2015-4176) CVE-2015-4176 kernel:deletion of a file or directory could unmount and reveal data under a mount point.	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1249442

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=e0c9c0afd2fc958ffa34b697972721d81df8a56f
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
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.0.2
mnt: Update detach_mounts to leave mounts connected · torvalds/linux@e0c9c0a · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/e0c9c0afd2fc958ffa34b697972721d81df8a56f

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→