CVE-2015-2925

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-2925
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-16 11:59:00 UTC
Updated	2018-01-05 02:30:00 UTC
Description	The prepend_path function in fs/dcache.c in the Linux kernel before 4.2.4 does not properly handle rename actions inside a

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
USN-2795-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
[security-announce] SUSE-SU-2016:0384-1: important: Security update for	SUSE	lists.opensuse.org
Linux Kernel CVE-2015-2925 Local Privilege Escalation Vulnerability	BID	www.securityfocus.c
Page not found :'(- src.fedoraproject.org	CONFIRM	pkgs.fedoraproject.c
USN-2798-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
[PATCH review 19/19] vfs: Do not allow escaping from bind mounts.	MLIST	permalink.gmane.or
[security-announce] SUSE-SU-2016:0386-1: important: Security update for	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
[security-announce] SUSE-SU-2016:0383-1: important: Security update for	SUSE	lists.opensuse.org
USN-2794-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
[security-announce] SUSE-SU-2016:0381-1: important: Security update for	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:0387-1: important: Security update for	SUSE	lists.opensuse.org

oss-security - Re: Linux namespaces: It is possible to escape from bind mounts	MLIST	www.openwall.com
Debian -- Security Information -- DSA-3364-1 linux	DEBIAN	www.debian.org
USN-2799-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
Bug 1209373 – CVE-2015-2925 Kernel: vfs: Do not allow escaping from bind mounts [fedora-all]	CONFIRM	bugzilla.redhat.com
[security-announce] SUSE-SU-2016:0380-1: important: Security update for	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2015:2194-1: important: Security update for	SUSE	lists.opensuse.org
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
vfs: Test for and handle paths that are unreachable from their mnt_root · torvalds/linux@397d425 · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Oracle Linux Bulletin - October 2015	CONFIRM	www.oracle.com
USN-2792-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
Oracle Linux Bulletin - January 2016	CONFIRM	www.oracle.com
[security-announce] SUSE-SU-2016:0337-1: important: Security update for	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:0434-1: important: Security update for	SUSE	lists.opensuse.org
[security-announce] SUSE-SU-2016:0335-1: important: Security update for	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-3372-1 linux	DEBIAN	www.debian.org
dcache: Handle escaped paths in prepend_path · torvalds/linux@cde93be · GitHub	CONFIRM	github.com
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.2.4	CONFIRM	www.kernel.org
[security-announce] SUSE-SU-2015:2292-1: important: Security update for	SUSE	lists.opensuse.org
permalink.gmane.org | 522: Connection timed out	MLIST	permalink.gmane.or
Bug 1209367 – CVE-2015-2925 Kernel: vfs: Do not allow escaping from bind mounts	CONFIRM	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.