CVE-2014-9731

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

Summary

CVE	CVE-2014-9731
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-31 10:59:00 UTC
Updated	2017-07-13 01:29:00 UTC
Description	The UDF filesystem implementation in the Linux kernel before 3.18.2 does not ensure that space is available for storing a s

Risk And Classification

Problem Types: CWE-17

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	Tags
Bug 1228220 – CVE-2014-9731 Kernel: fs: udf: information leakage when reading symlink	CONFIRM	bugzilla.redhat.com	
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.18.2	CONFIRM	www.kernel.org	Vendor A
[security-announce] SUSE-SU-2015:1224-1: important: Security update for	SUSE	lists.opensuse.org	
Android Security Bulletin—July 2017 | Android Open Source Project	CONFIRM	source.android.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	
[security-announce] SUSE-SU-2015:1611-1: important: Security update for	SUSE	lists.opensuse.org	
oss-security - CVE request Linux kernel: udf: information leakage when reading symlink	MLIST	www.openwall.com	
Linux Kernel CVE-2014-9731 Local Information Disclosure Vulnerability	BID	www.securityfocus.com	
[security-announce] openSUSE-SU-2015:1382-1: important: Security update	SUSE	lists.opensuse.org	
[security-announce] SUSE-SU-2015:1592-1: important: Security update for	SUSE	lists.opensuse.org	
[security-announce] SUSE-SU-2015:1324-1: important: Security update for	SUSE	lists.opensuse.org	
udf: Check path length when reading symlink · torvalds/linux@0e5cc9a · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**