CVE-2015-3202

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

Summary

CVE	CVE-2015-3202
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-02 21:59:00 UTC
Updated	2017-07-01 01:29:00 UTC
Description	fusermount in FUSE before 2.9.3-15 does not properly clear the environment before invoking (1) mount or (2) umount as ro

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Fuse Project	Fuse	All	All	All	All

References

Reference
Tavis Ormandy on Twitter: "a=/tmp/.$$;b=chmod\ u+sx;echo $b /bin/sh>$a;$b $a;a+=\;$a;mkdir -p $a;LIBMOUNT_MTAB=/etc/$0.$0rc _FUSE
USN-2617-1: FUSE vulnerability | Ubuntu
FUSE CVE-2015-3202 Local Privilege Escalation Vulnerability
[SECURITY] Fedora 20 Update: ntfs-3g-2015.3.14-2.fc20
openSUSE-SU-2015:1003-1: moderate: Security update for fuse
oss-security - CVE-2015-3202 fuse privilege escalation
USN-2617-3: NTFS-3G vulnerability | Ubuntu
Making a demo exploit for CVE-2015-3202 on Ubuntu fit in a tweet. · GitHub
[SECURITY] Fedora 21 Update: ntfs-3g-2015.3.14-2.fc21
[SECURITY] Fedora 22 Update: fuse-2.9.4-1.fc22
Filesystem in Userspace (FUSE) LIBMOUNT_MTAB Environment Variable Sanitization Flaw Lets Local Users Gain Elevated Privileges - Secu

Debian -- Security Information -- DSA-3268-1 ntfs-3g
FUSE: incorrect filtering of environment variables leading to privilege escalation (GLSA 201603-04) — Gentoo Security
Debian -- Security Information -- DSA-3266-1 fuse
Fuse Local Privilege Escalation ≈ Packet Storm
[SECURITY] Fedora 21 Update: fuse-2.9.4-1.fc21
Fuse 2.9.3-15 - Local Privilege Escalation - Linux local Exploit
openSUSE-SU-2015:0997-1: moderate: Security update for fuse
NTFS-3G: Privilege escalation (GLSA 201701-19) — Gentoo security
[SECURITY] Fedora 22 Update: ntfs-3g-2015.3.14-2.fc22
USN-2617-2: NTFS-3G vulnerability | Ubuntu
[SECURITY] Fedora 20 Update: fuse-2.9.4-1.fc20
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710449 Gentoo Linux NTFS-3G Privilege escalation Vulnerability (GLSA 201701-19)