CVE-2017-5551

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

Summary

CVE	CVE-2017-5551
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-06 06:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The simple_set_acl function in fs/posix_acl.c in the Linux kernel before 4.9.6 preserves the setgid bit during a setxattr call ir

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
tmpfs: clear S_ISGID when setting posix ACLs · torvalds/linux@497de07 · GitHub	CONFIRM
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.6	CONFIRM
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
Linux Kernel 'tmpfs' File System Permission Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRA
oss-security - Re: CVE REQUEST: linux kernel: process with pgid zero able to crash kernel	MLIST
Bug 1416126 – CVE-2017-5551 kernel: S_ISGD is not cleared when setting posix ACLs in tmpfs (CVE-2016-7097 incomplete fix)	CONFIRM
Debian -- Security Information -- DSA-3791-1 linux	DEBIAN
Linux Kernel CVE-2017-5551 Local Denial of Service Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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**