CVE-2016-7916

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-7916
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-16 05:59:00 UTC
Updated	2017-01-18 02:59:00 UTC
Description	Race condition in the environ_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain se

Risk And Classification

Problem Types: CWE-362

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
proc: prevent accessing /proc/<PID>/environ until it's ready · torvalds/linux@8148a73 · GitHub	CONFIRM	github.com	Issue
Android Security Bulletin—November 2016 | Android Open Source Project	CONFIRM	source.android.com	Third
USN-3159-1: Linux kernel vulnerability | Ubuntu	UBUNTU	www.ubuntu.com	
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.4	CONFIRM	www.kernel.org	Relea
grsecurity forums • View topic - PAX: size overflow in function environ_read fs/proc/base.c	CONFIRM	forums.grsecurity.net	Issue
Linux Kernel Multiple Information Disclosure Vulnerabilities	BID	www.securityfocus.com	Third
Bug 116461 – PAX: size overflow in function environ_read fs/proc/base.c	CONFIRM	bugzilla.kernel.org	Issue
USN-3159-2: Linux kernel (OMAP4) vulnerability | Ubuntu	UBUNTU	www.ubuntu.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Issue
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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

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