CVE-2017-9150

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

Summary

CVE	CVE-2017-9150
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-22 22:29:00 UTC
Updated	2017-09-09 01:29:00 UTC
Description	The do_check function in kernel/bpf/verifier.c in the Linux kernel before 4.11.1 does not make the allow_ptr_leaks value ava

Risk And Classification

Problem Types: CWE-200

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	Tag
Android Security Bulletin—September 2017 | Android Open Source Project	CONFIRM	source.android.com	
Linux Kernel CVE-2017-9150 Local Information Disclosure Vulnerability	BID	www.securityfocus.com	
bpf: don't let ldimm64 leak map addresses on unprivileged · torvalds/linux@0d0e576 · GitHub	MISC	github.com	Iss
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Iss
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.11.1	MISC	www.kernel.org	Rel
1251 - Linux: eBPF verifier log leaks lower half of map pointer - project-zero - Monorail	MISC	bugs.chromium.org	Iss
Linux Kernel 4.11 - eBPF Verifier Log Leaks Lower Half of map Pointer	EXPLOIT-DB	www.exploit-db.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

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