



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 av

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	Tags
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	Issue
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Issue
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.11.1	MISC	www.kernel.org	Release
1251 - Linux: eBPF verifier log leaks lower half of map pointer - project-zero - Monorail	MISC	bugs.chromium.org	Issue
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	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)