



CVE-2015-8967

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2015-8967
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-08 21:59:00 UTC
Updated	2023-01-19 16:07:00 UTC
Description	arch/arm64/kernel/sys.c in the Linux kernel before 4.0 allows local users to bypass the "strict page permissions" protection

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
Linux Kernel CVE-2015-8967 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com	
Android Security Bulletin—December 2016 Android Open Source Project	CONFIRM	source.android.com	Third Party Advisory
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Issue Tracking, Patch, Ve
arm64: make sys_call_table const · torvalds/linux@c623b33 · GitHub	CONFIRM	github.com	Issue Tracking, Patch, Th
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[671047](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

© [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](#).

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