



CVE-2015-8966

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

Summary

CVE	CVE-2015-8966
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-08 21:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OF

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.001820000 probability, percentile 0.395630000 (date 2026-05-10)

Problem Types: CWE-264 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Li
[PATCH] arm: fix handling of F_OFD_... in oabi_fcntl64() · torvalds/linux@76cc404 · GitHub	af854a3a-2127-422b-91ae-364da2661108	git
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da2661108	git
Linux Kernel CVE-2015-8966 Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da2661108	wn
Android Security Bulletin—December 2016 Android Open Source Project	af854a3a-2127-422b-91ae-364da2661108	sc
CVE Program record	CVE.ORG	wn
NVD vulnerability detail	NVD	nv

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](#)