



CVE-2016-8440

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

Summary

CVE	CVE-2016-8440
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-12 20:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Possible buffer overflow in SMMU system call. Improper input validation in ADSP SID2CB system call may result in hypervi

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.005320000 probability, percentile 0.673620000 (date 2026-05-08)

Problem Types: CWE-119 | Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/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	3.18	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Inc.	Android	affected Kernel-3.18	Not specified

References

Reference	Source	Link
Android Security Bulletin—January 2017 Android Open Source Project	af854a3a-2127-422b-91ae-364da2661108	source.android.com
Google Android Qualcomm components Multiple Unspecified Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.security.google.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)