CVE-2016-8445

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

Summary

CVE	CVE-2016-8445
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-12 20:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	An elevation of privilege vulnerability in MediaTek components, including the thermal driver and video driver, could enable a

Risk And Classification

Primary CVSS: v3.0 7 HIGH from nvd@nist.gov

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

EPSS: 0.000490000 probability, percentile 0.151450000 (date 2026-05-10)

Problem Types: CWE-264 | Elevation of privilege

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7	HIGH	CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.6		AV:N/AC:H/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Inc.	Android	affected n/a	Not specified

References

Reference	Source	Link
Google Android MediaTek Components Multiple Privilege Escalation Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.secu
Android Security Bulletin—January 2017 | Android Open Source Project	af854a3a-2127-422b-91ae-364da2661108	source.and
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

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