



# CVE-2017-0435

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

## Summary

|                 |                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2017-0435                                                                                                                 |
| State           | PUBLISHED                                                                                                                     |
| Assigner        | google_android                                                                                                                |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                  |
| Published       | 2017-02-08 15:59:01 UTC                                                                                                       |
| Updated         | 2025-04-20 01:37:25 UTC                                                                                                       |
| Description     | An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute ar |

## 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

Problem Types: NVD-CWE-noinfo | 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      |
| Operating System | Linux  | Linux Kernel | 3.10    | All    | All     | All      |
| 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-3.10 | Not specified |
| CNA    | Google Inc. | Android | affected Kernel-3.18 | Not specified |

#### References

##### Reference

Google Nexus/ Pixel Products Qualcomm Sound Driver Multiple Privilege Escalation Vulnerabilities

Android Security Bulletin—February 2017 | Android Open Source Project

Google Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remot

CVE Program record

NVD vulnerability detail

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](#)