



# CVE-2016-2452

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

| Summary         |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-2452                                                                                                               |
| State           | PUBLISHED                                                                                                                   |
| Assigner        | google_android                                                                                                              |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                |
| Published       | 2016-05-09 10:59:30 UTC                                                                                                     |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                     |
| Description     | codecs/amrnb/dec/SoftAMR.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before |

Risk And Classification

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

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

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:N/UI:R/S:U/C:H/I:H/A:H |
| 2.0     | nvd@nist.gov | Primary | 9.3   |          | AV:N/AC:M/Au:N/C:C/I:C/A:C                   |

| CVSS v3.0 Breakdown |           |
|---------------------|-----------|
| Attack Vector       | Local     |
| Attack Complexity   | Low       |
| Privileges Required | None      |
| User Interaction    | Required  |
| Scope               | Unchanged |
| Confidentiality     | High      |
| Integrity           | High      |
| Availability        |           |

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/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 | 4.0     | All    | All     | All      |
| Operating System | Google | Android | 4.0.1   | All    | All     | All      |
| Operating System | Google | Android | 4.0.2   | All    | All     | All      |
| Operating System | Google | Android | 4.0.3   | All    | All     | All      |
| Operating System | Google | Android | 4.0.4   | All    | All     | All      |
| Operating System | Google | Android | 4.1     | All    | All     | All      |
| Operating System | Google | Android | 4.1.2   | All    | All     | All      |
| Operating System | Google | Android | 4.2     | All    | All     | All      |
| Operating System | Google | Android | 4.2.1   | All    | All     | All      |
| Operating System | Google | Android | 4.2.2   | All    | All     | All      |
| Operating System | Google | Android | 4.3     | All    | All     | All      |
| Operating System | Google | Android | 4.3.1   | All    | All     | All      |
| Operating System | Google | Android | 4.4     | All    | All     | All      |
| Operating System | Google | Android | 4.4.1   | All    | All     | All      |
| Operating System | Google | Android | 4.4.2   | All    | All     | All      |
| Operating System | Google | Android | 4.4.3   | All    | All     | All      |
| Operating System | Google | Android | 5.0     | All    | All     | All      |

|                  |                        |                         |       |     |     |     |
|------------------|------------------------|-------------------------|-------|-----|-----|-----|
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 5.0.1 | All | All | All |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 5.1   | All | All | All |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 5.1.0 | All | All | All |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 6.0   | All | All | All |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 6.0.1 | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |  |

| References                                                                        |  |  |                                      |  |                     |  |
|-----------------------------------------------------------------------------------|--|--|--------------------------------------|--|---------------------|--|
| Reference                                                                         |  |  | Source                               |  | Link                |  |
| daa85dac2055b22dabbb3b4e537597e6ab73a866 - platform/frameworks/av - Git at Google |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">an</a>  |  |
| 65756b4082cd79a2d99b2ccb5b392291fd53703f - platform/frameworks/av - Git at Google |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">an</a>  |  |
| 44749eb4f273f0eb681d0fa013e3beef754fa687 - platform/frameworks/av - Git at Google |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">an</a>  |  |
| Android Security Bulletin—May 2016   Android Open Source Project                  |  |  | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">so</a>  |  |
| CVE Program record                                                                |  |  | CVE.ORG                              |  | <a href="#">ww</a>  |  |
| NVD vulnerability detail                                                          |  |  | NVD                                  |  | <a href="#">nvd</a> |  |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.