



# CVE-2016-3916

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

## Summary

|                 |                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2016-3916                                                                                                                                                                                                                           |
| State           | PUBLISHED                                                                                                                                                                                                                               |
| Assigner        | google_android                                                                                                                                                                                                                          |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                                                                                                            |
| Published       | 2016-10-10 10:59:20 UTC                                                                                                                                                                                                                 |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                                                                                                                                 |
| Description     | camera/src/camera_metadata.c in the Camera service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 6.0.1, and 7.x before 7.0.0 allows an attacker to read arbitrary memory via a crafted camera applet. |

## 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

**EPSS:** 0.000590000 probability, percentile 0.183300000 (date 2026-05-07)

**Problem Types:** CWE-119 | 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

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 | <a href="#">Google</a> | <a href="#">Android</a> | 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 |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 7.0   | All | All | All |

| Vendor Declared Affected Products |        |         |              |               |  |  |
|-----------------------------------|--------|---------|--------------|---------------|--|--|
| Source                            | Vendor | Product | Version      | Platforms     |  |  |
| CNA                               | Na     | N/a     | affected n/a | Not specified |  |  |

| References                                                                       |                                      |  |                        |
|----------------------------------------------------------------------------------|--------------------------------------|--|------------------------|
| Reference                                                                        | Source                               |  | Link                   |
| Android Security Bulletin—October 2016   Android Open Source Project             | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">source</a> |
| Google Android Camera Service Multiple Privilege Escalation Vulnerabilities      | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">www</a>    |
| 8e7a2b4d13bff03973dbad2bfb88a04296140433 - platform/system/media - Git at Google | af854a3a-2127-422b-91ae-364da2661108 |  | <a href="#">andri</a>  |
| CVE Program record                                                               | CVE.ORG                              |  | <a href="#">www</a>    |
| NVD vulnerability detail                                                         | NVD                                  |  | <a href="#">nvd.r</a>  |

No vendor comments have been submitted for this CVE.

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