



# CVE-2017-0483

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-0483                                                                                                                   |
| <b>State</b>           | PUBLIC                                                                                                                          |
| <b>Assigner</b>        | security@android.com                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                    |
| <b>Published</b>       | 2017-03-08 01:59:00 UTC                                                                                                         |
| <b>Updated</b>         | 2017-07-17 13:18:00 UTC                                                                                                         |
| <b>Description</b>     | A denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device har |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                 | Version | Update | Edition | Language |
|------------------|------------------------|-------------------------|---------|--------|---------|----------|
| 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> | 5.0.2   | 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> | 5.1.1   | 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      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 7.1.0   | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 7.1.1   | 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> | 5.0.2   | 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> | 5.1.1   | 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 |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 7.1.0 | All | All | All |
| Operating System | <a href="#">Google</a> | <a href="#">Android</a> | 7.1.1 | All | All | All |

References

| Reference                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------|
| Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users |
| Google Android Mediaserver Multiple Denial of Service Vulnerabilities                                                                      |
| Android Security Bulletin—March 2017   Android Open Source Project                                                                         |
| Android Security Bulletin—March 2017   Android Open Source Project                                                                         |
| 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.