



CVE-2016-3898

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

Summary

CVE	CVE-2016-3898
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-11 21:59:43 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Telephony in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows attack

Risk And Classification

Primary CVSS: v3.0 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000670000 probability, percentile 0.204670000 (date 2026-05-06)

Problem Types: CWE-284 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	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
d1d248d10cf03498efb7041f1a8c9c467482a19d - platform/packages/services/Telephony - Git at Google
Android Security Bulletin—September 2016 Android Open Source Project
Google Android Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code and Let Applications Obtain Potentially Sensitive

CVE.report and Source URL Uptime Status status.cve.report