CVE-2017-0640

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

Summary

CVE	CVE-2017-0640
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-14 13:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	A remote denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a de

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

Problem Types: NVD-CWE-noinfo | Denial of service

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

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

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Operating System	Google	Android	7.1.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Inc.	Android	affected Android-6.0 Android-6.0.1 Android-7.0 Android-7.1.1	Not specified

References

Reference
Google Android Media Framework Multiple Memory Corruption Vulnerabilities
Android Security Bulletin—June 2017 | Android Open Source Project
Google Android Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Execute Arbitrary Code and Let
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.

Free CVE JSON API cve.report/api

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