



CVE-2015-3829

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

Summary

CVE	CVE-2015-3829
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-01 00:59:00 UTC
Updated	2017-09-21 01:29:00 UTC
Description	Off-by-one error in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Google Android MMS Media Processing Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SECTRA
Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities	BID
Security Advisory - Stagefright Vulnerability in Multiple Huawei Android Products	CONFIRMED
2674a7218eaa3c87f2ee26d26da5b9170e10f859 - platform/frameworks/av - Git at Google	CONFIRMED
Security Advisory - Stagefright Vulnerability in Multiple Huawei Android Products	CONFIRMED
[android-security-updates] 20150812 Nexus Security Bulletin (August 2015)	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)