CVE-2015-3827

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

Summary

CVE	CVE-2015-3827
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-01 00:59:11 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does n

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-119 | CWE-189 | n/a

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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities	af854a3a
f4a88c8ed4f8186b3d6e2852993e063fc33ff231 - platform/frameworks/av - Git at Google	af854a3a
Security Advisory - Stagefright Vulnerability in Multiple Huawei Android Products	af854a3a
Security Advisory - Stagefright Vulnerability in Multiple Huawei Android Products	af854a3a
Google Android MMS Media Processing Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	af854a3a
groups.google.com/forum/message/raw	af854a3a
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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