



CVE-2015-3864

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

Summary

CVE	CVE-2015-3864
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-01 00:59:00 UTC
Updated	2017-09-16 01:29:00 UTC
Description	Integer underflow in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in mediaserver in A

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	Link
Reflecting on Stagefright Patches › Zimperium Mobile Security Blog	MISC	blog.zimperium.com
Google Android 5.0 < 5.1.1 - 'Stagefright' .MP4 tx3g Integer Overflow (Metasploit) - Android remote Exploit	EXPLOIT-DB	www.exploit-db.com
Android libstagefright - Integer Overflow Remote Code Execution	EXPLOIT-DB	www.exploit-db.com
6fe85f7e15203e48df2cc3e8e1c4bc6ad49dc968 - platform/frameworks/av - Git at Google	CONFIRM	android.googlesource.com
CVE-2015-3864 Metasploit module now available for testing › Zimperium Mobile Security Blog	MISC	blog.zimperium.com
Google Android Stagefright CVE-2015-3864 Incomplete Fix Integer Overflow Vulnerability	BID	www.securityfocus.com
Google Android 5.0.1 - Metaphor Stagefright (ASLR Bypass) - Android remote Exploit	EXPLOIT-DB	www.exploit-db.com
Android Open Source Project = Details	MLIST	groups.google.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)