



CVE-2016-0840

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

Summary

CVE	CVE-2016-0840
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-18 00:59:00 UTC
Updated	2016-04-20 16:41:00 UTC
Description	Multiple stack-based buffer underflows in decoder/ih264d_parse_cavlc.c in mediaserver in Android 6.x before 2016-04-01 a

Risk And Classification

Problem Types: CWE-119

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	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All

References

Reference	Source	Link	Tags
c57fc3703ae2e0d41b1f6580c50015937f2d23c1 - platform/external/libavc - Git at Google	CONFIRM	android.googlesource.com	Vendor
Nexus Security Bulletin—April 2016 Android Open Source Project	CONFIRM	source.android.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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](#)