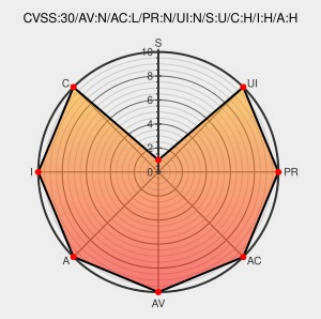
CVE-2016-2428

Published on: 05/09/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:15 PM UTC

CVE-2016-2428

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Android from Google contain the following vulnerability:

libAACdec/src/aacdec_drc.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not properly limit the number of threads, which allows remote attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via a crafted media file, aka internal bug 26751339.

CVE-2016-2428 has been assigned by security@android.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
5d4405f601fa11a8955fd7611532c982420e4206 - platform/external/aac - Git at Google	android.googlesource.com text/html	CONFIRM android.googlesource.com/platform/external/aac/+/5d4405f601f

Android Security Bulletin—May 2016 | Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-05-01.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All

Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All

Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All

cpe:2.3:o:google:android:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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