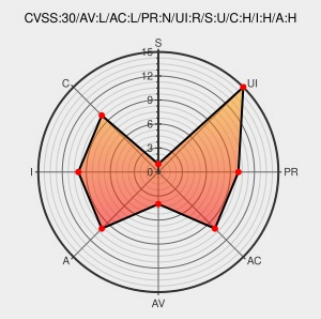
CVE-2016-2487

Published on: 06/12/2016 12:00:00 AM UTC

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

CVE-2016-2487

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



Certain versions of Android from Google contain the following vulnerability:

libstagefright 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 2016-06-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27833616.

CVE-2016-2487 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
4e32001e4196f39ddd0b86686ae0231c8f5ed944 - platform/frameworks/av - Git at Google	android.googlesource.com, text/html	CONFIRM android.googlesource.com/platform/frameworks/av/+/4e32001e
Android Security Bulletin—June 2016 | Android Open Source Project	Vendor Advisory, source.android.com	CONFIRM source.android.com/security/bulletin/2016-06-01

	text/html	
918eeaa29d99d257282fafec931b4bda0e3bae12 - platform/frameworks/av - Git at Google	android.googlesource.com text/html	CONFIRM android.googlesource.com/platform/frameworks/av/+/918eeaa2
d2f47191538837e796e2b10c1ff7e1ee35f6e0ab - platform/frameworks/av - Git at Google	android.googlesource.com text/html	CONFIRM android.googlesource.com/platform/frameworks/av/+/d2f47191

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	4.1.1	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	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	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	4.1.1	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	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	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:4.0.2:*:*:*:*:*:*:*:

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:4.1.1:*:*:*:*:*:*:*:

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: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: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:4.1.1:*:*:*:*:*:*:*:

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: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:6.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→