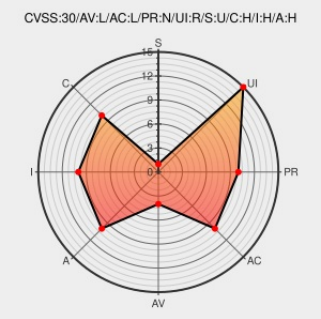
CVE-2017-0381

Published on: 01/12/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:52 PM UTC

CVE-2017-0381

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



Certain versions of Android from Google contain the following vulnerability:

An information disclosure vulnerability in silk/NLSF_stabilize.c in libopus in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1. Android ID: A-31607432.

CVE-2017-0381 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
About the security content of macOS High Sierra 10.13 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/HT208144

About the security content of watchOS 4 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/HT208115
Android Security Bulletin—January 2017 | Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2017-01-01
Google Android Mediaserver CVE-2017-0381 Remote Code Execution Vulnerability	cve.report (archive) text/html	BID 95248
Opus: User-assisted execution of arbitrary code (GLSA 201702-21) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201702-21
About the security content of iOS 11 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/HT208112
Apple macOS/OS X Multiple Flaws Let Remote and Local Users Bypass Security and Deny Service, Local Users Obtain Potentially Sensitive Information, and Applications Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1039427
0d052d64480a30e83fcdda80f4774624e044beb7 - platform/external/libopus - Git at Google	Issue Tracking Patch android.googlesource.com text/html	CONFIRM android.googlesource.com/platform/external/libopus/+/0d052d6
About the security content of tvOS 11 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/HT208113

Related QID Numbers

710341 Gentoo Linux Opus User-assisted execution of arbitrary code Vulnerability (GLSA 201702-21)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.0.2	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	5.1.1	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	7.0	All	All	All
Operating System	Google	Android	7.1.0	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	5.0.2	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	5.1.1	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	7.0	All	All	All
Operating System	Google	Android	7.1.0	All	All	All

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

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

cpe:2.3:o:google:android:5.0.2:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:5.1.1:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.1.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:5.0.2:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:5.1.1:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→