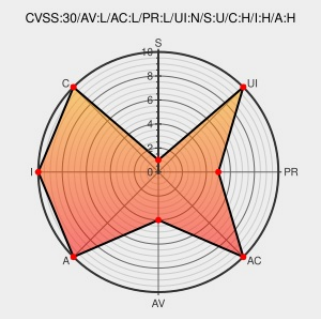
CVE-2017-15845

Published on: 01/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:32 PM UTC

CVE-2017-15845

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



Certain versions of Android from Google contain the following vulnerability:

In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, an invalid input of firmware size (negative value) from user space can potentially lead to the memory leak or buffer overflow during the WLAN cal data store operation.

CVE-2017-15845 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Qualcomm, Inc.** - **Android for MSM, Firefox OS for MSM, QRD Android** version **All Android releases from CAF using the Linux kernel**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Pixel/Nexus Security Bulletin—January 2018 | Android Open Source Project	Patch Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2018-01-01

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	-	All	All	All
Operating System	Google	Android	-	All	All	All

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→