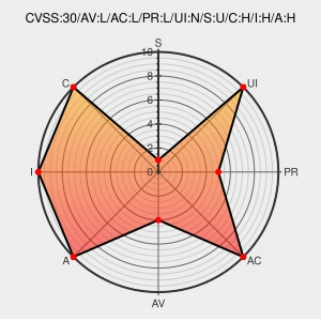
CVE-2017-15831

Published on: 03/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15831

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, in the function wma_ndp_end_indication_event_handler(), there is no input validation check on a event_info value coming from firmware, which can cause an integer overflow and then leads to potential heap overwrite.

CVE-2017-15831 has been assigned by product-security@qualcomm.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	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
platform/vendor/qcom-opensource/wlan/qcacld-3.0 - Unnamed	Patch Third Party Advisory	MISC source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?

repository	source.codeaurora.org text/html	id=31e6a6573206429c6596d57d38a69afe8c1ce1
Pixel/Nexus Security Bulletin—March 2018 | Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2018-03-01

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→