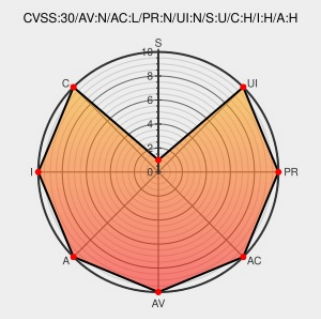
CVE-2017-14876

Published on: 03/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14876

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



Certain versions of Android from Google contain the following vulnerability:

In msm_ispif_config_stereo() in Android for MSM, Firefox OS for MSM, and QRD Android before 2017-06-21, the parameter params->entries[i].vfe_intf comes from userspace without any bounds check which could potentially result in a kernel out-of-bounds write.

CVE-2017-14876 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as CRITICAL 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: 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: 7.5 - HIGH

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

CVE References

Description	Tags	Link
kernel/msm-3.18 - Unnamed repository; edit this file	Patch	MISC source.codeaurora.org/quic/la/kernel/msm-

'description' to name the repository.	Third Party Advisory source.codeaurora.org text/html	3.18/commit/? id=f26dbd9d9491333766ba383044064b1304127ac0
Pixel/Nexus Security Bulletin—February 2018 | Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2018-02-01

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→