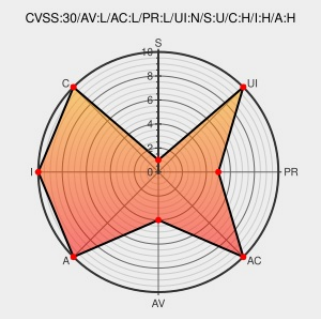
CVE-2018-11298

Published on: 09/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11298

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



Certain versions of Android from Google contain the following vulnerability:

In all android releases (Android for MSM, Firefox OS for MSM, QRD Android) from CAF using the linux kernel, while processing SET_PASSPOINT_LIST vendor command HDD does not make sure that the realm string that gets passed by upper-layer is NULL terminated. This may lead to buffer overflow as strlen is used to get realm string length to construct the PASSPOINT WMA command.

CVE-2018-11298 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
September 2018 Code Aurora Security Bulletin - Code Aurora	Patch Third Party Advisory www.codeaurora.org text/html	CONFIRM www.codeaurora.org/security-bulletin/2018/09/04/september-2018-code-aurora-security-bulletin
platform/vendor/qcom-opensource/wlan/qcacld-3.0 - Unnamed repository	Patch Third Party Advisory source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=9074c6cfb9c0bbfe279394eec0d3176c4f75ce80
Pixel/Nexus Security Bulletin—September 2018	Patch Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2018-09-01#qualcomm-components

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→