



CVE-2018-11298

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

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

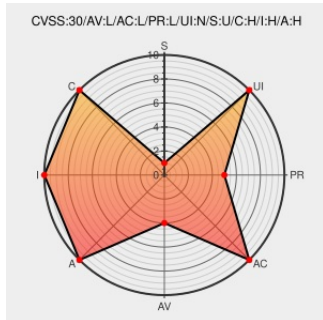
CVE-2018-11298

[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 [Q](#) product-security@qualcomm.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Q](#) 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
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report .		

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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)