

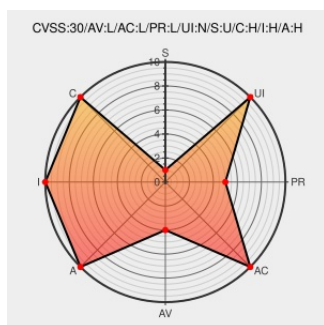


# CVE-2017-15823

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

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

## CVE-2017-15823

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

In `spectral_create_samp_msg()` in Android for MSM, Firefox OS for MSM, and QRD Android before 2017-10-11, some values from firmware are not properly validated potentially leading to a buffer overflow.

CVE-2017-15823 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                                                                     |
|---------------------------------------|-----------------------|--------------------------------------------------------------------------|
| <a href="#">platform/vendor/qcom-</a> | <a href="#">Patch</a> | <a href="#">MISC source.codeaurora.org/quic/la/platform/vendor/qcom-</a> |

platform/vendor/qcom/opensource/wlan/qcacld-3.0 - Unnamed repository

Third Party Advisory

source.codeaurora.org

text/html

platform/vendor/qcom/opensource/wlan/qcacld-3.0/commit/?id=49c1ce19c8a4689c33e6e8f17ab77d77fae6ff93

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

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](mailto: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