



# CVE-2018-11832

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

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

## CVE-2018-11832

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

CVSS:30/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



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, lack of input size validation before copying to buffer in PMIC function can lead to heap overflow.

CVE-2018-11832 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                                                              |
|-------------------------------------------------|-----------------------|-------------------------------------------------------------------|
| kernel/msm-3.18 - Unnamed repository: edit this | <a href="#">Patch</a> | <a href="#">CONFIRM source codeaurora.org/quic/la/kernel/msm-</a> |

Repository: [Enhanced repository](#); set the file 'description' to name the repository.

Patch

Third Party Advisory

source.codeaurora.org

text/html

CONFIRM

3.18/commit/?id=492fdce2626efc01004bea4aed4ea89b7c5cb5b3

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

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