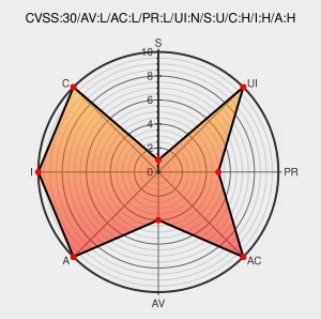
CVE-2017-18159

Published on: 07/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18159

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



Certain versions of Android from Google contain the following vulnerability:

In Android releases from CAF using the linux kernel (Android for MSM, Firefox OS for MSM, QRD Android) before security patch level 2018-06-05, while processing a StrHwPlatform with length smaller than EFICHIPINFO_MAX_ID_LENGTH, an array out of bounds access may occur.

CVE-2017-18159 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: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=04f23441b8c0c897644f9bf391b691039fa0ab70
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=b6b318431983f35a7734cae227478df3dc93a818
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=5471b0cdf4bace12d872d074b97eae29f1317e6a
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=7dcbee530800b16534d0f3e8db375492c03b3e0a
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=bcceb2ceeea07aedaa5f97207cc88f9d8b4416ea
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=4a63a848c062851776123d4bc7ec10eb498a70dd
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=3129148e5a4cfe83003449a1048660823bfddc51
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=633fa4ffb38bbfb0fad79204e19b9f59d42d7680
Android Security Bulletin—June 2018 | Android Open Source Project	Patch Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2018-06-01#qualcomm-components
abl/tianocore/edk2 - Unnamed repository	Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/?id=9057a8b3339abc4eb2c4e462279f34bbe6410e7c

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 registred 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