



CVE-2017-18302

Published on: 09/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:54 PM UTC

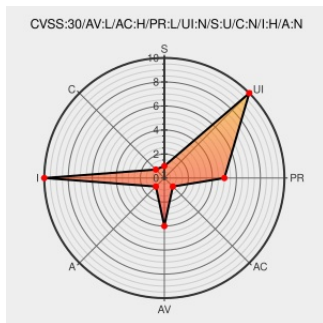
CVE-2017-18302

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Msm8996au](#) from [Qualcomm](#) contain the following vulnerability:

In Snapdragon (Automobile ,Mobile) in version MSM8996AU, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 650/52, SD 820, SD 820A, SD 835, SDA660, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, Snapdragon_High_Med_2016, a crafted HLOS client can modify the structure in memory passed to a QSEE

application between the time of check and the time of use, resulting in arbitrary writes to TZ kernel memory regions.

CVE-2017-18302 has been assigned by [Q](#) product-security@qualcomm.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Q](#) **Qualcomm, Inc. - Snapdragon Automobile, Snapdragon Mobile** version **MSM8996AU, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 650/52, SD 820, SD 820A, SD 835, SDA660, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, Snapdragon_High_Med_2016**

CVSS3 Score: **4.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **4.7 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	COMPLETE	NONE

CVE References

Description	Tags	Link
Android Security Bulletin—August 2018 Android Open Source Project	Vendor Advisory source.android.com text/html	 CONFIRM source.android.com/security/bulletin/2018-08-01#qualcomm-closed-source-components
Google Android Multiple Flaws Let Remote Users Execute Arbitrary Code and Let Applications Gain Elevated Privileges and Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRACK 1041432
Bulletins Qualcomm	Vendor Advisory www.qualcomm.com text/html	 CONFIRM www.qualcomm.com/company/product-security/bulletins

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
Hardware 	Qualcomm	Msm8996au	-	All	All	All
Hardware 	Qualcomm	Msm8996au	-	All	All	All
Operating System	Qualcomm	Msm8996au Firmware	-	All	All	All
Operating System	Qualcomm	Msm8996au Firmware	-	All	All	All
Hardware 	Qualcomm	Sd425	-	All	All	All
Hardware 	Qualcomm	Sd425	-	All	All	All
Operating System	Qualcomm	Sd425 Firmware	-	All	All	All
Operating System	Qualcomm	Sd425 Firmware	-	All	All	All
Hardware 	Qualcomm	Sd427	-	All	All	All
Hardware 	Qualcomm	Sd427	-	All	All	All
Operating System	Qualcomm	Sd427 Firmware	-	All	All	All
Operating System	Qualcomm	Sd427 Firmware	-	All	All	All
Hardware 	Qualcomm	Sd430	-	All	All	All
Hardware 	Qualcomm	Sd430	-	All	All	All

Operating System	Qualcomm	Sd820a Firmware	-	All	All	All
Operating System	Qualcomm	Sd820a Firmware	-	All	All	All
Operating System	Qualcomm	Sd820 Firmware	-	All	All	All
Operating System	Qualcomm	Sd820 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd835	-	All	All	All
Hardware  	Qualcomm	Sd835	-	All	All	All
Operating System	Qualcomm	Sd835 Firmware	-	All	All	All
Operating System	Qualcomm	Sd835 Firmware	-	All	All	All
Hardware  	Qualcomm	Sda660	-	All	All	All
Hardware  	Qualcomm	Sda660	-	All	All	All
Operating System	Qualcomm	Sda660 Firmware	-	All	All	All
Operating System	Qualcomm	Sda660 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm429	-	All	All	All
Hardware  	Qualcomm	Sdm429	-	All	All	All
Operating System	Qualcomm	Sdm429 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm429 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm439	-	All	All	All
Hardware  	Qualcomm	Sdm439	-	All	All	All
Operating System	Qualcomm	Sdm439 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm439 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm630	-	All	All	All
Hardware  	Qualcomm	Sdm630	-	All	All	All
Operating System	Qualcomm	Sdm630 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm630 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm632	-	All	All	All
Hardware  	Qualcomm	Sdm632	-	All	All	All
Operating	Qualcomm	Sdm632 Firmware	-	All	All	All

System						
Operating System	Qualcomm	Sdm632 Firmware	-	All	All	All
Hardware	Qualcomm	Sdm636	-	All	All	All
Hardware	Qualcomm	Sdm636	-	All	All	All
Operating System	Qualcomm	Sdm636 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm636 Firmware	-	All	All	All
Hardware	Qualcomm	Sdm660	-	All	All	All
Hardware	Qualcomm	Sdm660	-	All	All	All
Operating System	Qualcomm	Sdm660 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm660 Firmware	-	All	All	All
<code>cpe:2.3:h:qualcomm:msm8996au:-:*:*:*:*:*:</code>						
<code>cpe:2.3:h:qualcomm:msm8996au:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:qualcomm:msm8996au_firmware:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:qualcomm:msm8996au_firmware:-:*:*:*:*:*:</code>						
<code>cpe:2.3:h:qualcomm:sd425:-:*:*:*:*:*:</code>						
<code>cpe:2.3:h:qualcomm:sd425:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:qualcomm:sd425_firmware:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:qualcomm:sd425_firmware:-:*:*:*:*::~:</code>						
<code>cpe:2.3:h:qualcomm:sd427:-:*:*:*:*:*:</code>						
<code>cpe:2.3:h:qualcomm:sd427:-:*:*:*:*::~:</code>						
<code>cpe:2.3:o:qualcomm:sd427_firmware:-:*:*:*:*::~:</code>						
<code>cpe:2.3:o:qualcomm:sd427_firmware:-:*:*:*:*::~:</code>						
<code>cpe:2.3:h:qualcomm:sd430:-:*:*:*:*::~:</code>						
<code>cpe:2.3:h:qualcomm:sd430:-:*:*:*:*::~:</code>						
<code>cpe:2.3:o:qualcomm:sd430_firmware:-:*:*:*:*::~:</code>						
<code>cpe:2.3:o:qualcomm:sd430_firmware:-:*:*:*:*::~:</code>						
<code>cpe:2.3:h:qualcomm:sd435:-:*:*:*:*::~:</code>						
<code>cpe:2.3:h:qualcomm:sd435:-:*:*:*:*::~:</code>						

```
cpe:2.3:o:qualcomm:sd435_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd435_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd450:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd450:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd450_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd450_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd625:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd625:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd625_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sd625_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd650:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd650:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd650 firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd650_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd652:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd652:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sd652_firmware:-:*:*:*:*:*

```
cpe:2.3:o:qualcomm:sd652 firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd820:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd820:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd820a:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd820a:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd820a_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sd820a_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sd820_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd820_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd835:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd835:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd835_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd835_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sda660:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sda660:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sda660_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sda660_firmware:-:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm429:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm429:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm429_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm429_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm439:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm439:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm439 firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sdm439_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:h:qualcomm:sdm630:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm630:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm630_firmware:-:*:*:*:*:*.*
```

```
cpe:2.3:o:qualcomm:sdm630_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm632:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm632:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm632 firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sdm632 firmware:-.*:.*:.*:.*:.*:.*
```

cpe:2.3:h:qualcomm:sdm636:-:*:*:*:*:*:*:

```
cpe:2.3:h:qualcomm:sdm636:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm636_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm636_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:h:qualcomm:sdm660:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm660:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm660_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:o:qualcomm:sdm660_firmware:-:*:*:*:*:*:

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](#)