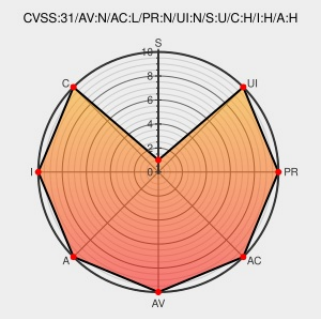
CVE-2020-11153

Published on: 11/02/2020 12:00:00 AM UTC

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

CVE-2020-11153

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



Certain versions of Apq8053 from Qualcomm contain the following vulnerability:

u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55

CVE-2020-11153 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Qualcomm, Inc.** - **Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile** version **APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
October 2020 Security Bulletin | Qualcomm	Vendor Advisory www.qualcomm.com text/html	MISC www.qualcomm.com/company/product-security/bulletins/october-2020-security-bulletin
Page not found	Broken Link www.qualcomm.com text/html Inactive Link Not Archived	CONFIRM www.qualcomm.com/company/product-security/bulletins/october-2020-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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Qualcomm	Apq8053	-	All	All	All
Hardware	Qualcomm	Apq8053	-	All	All	All
Operating System	Qualcomm	Apq8053 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8053 Firmware	-	All	All	All
Hardware	Qualcomm	Qca6390	-	All	All	All
Hardware	Qualcomm	Qca6390	-	All	All	All
Operating System	Qualcomm	Qca6390 Firmware	-	All	All	All
Operating System	Qualcomm	Qca6390 Firmware	-	All	All	All
Hardware	Qualcomm	Qca9379	-	All	All	All
Hardware	Qualcomm	Qca9379	-	All	All	All
Operating System	Qualcomm	Qca9379 Firmware	-	All	All	All
Operating System	Qualcomm	Qca9379 Firmware	-	All	All	All
Hardware	Qualcomm	Qcn7605	-	All	All	All
Hardware	Qualcomm	Qcn7605	-	All	All	All
Operating System	Qualcomm	Qcn7605 Firmware	-	All	All	All
Operating System	Qualcomm	Qcn7605 Firmware	-	All	All	All

Hardware	Qualcomm	Sc8180x	-	All	All	All
Hardware	Qualcomm	Sc8180x	-	All	All	All
Operating System	Qualcomm	Sc8180x Firmware	-	All	All	All
Operating System	Qualcomm	Sc8180x Firmware	-	All	All	All
Hardware	Qualcomm	Sdx55	-	All	All	All
Hardware	Qualcomm	Sdx55	-	All	All	All
Operating System	Qualcomm	Sdx55 Firmware	-	All	All	All
Operating System	Qualcomm	Sdx55 Firmware	-	All	All	All

cpe:2.3:h:qualcomm:apq8053:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:apq8053:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:apq8053_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:apq8053_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca6390:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca6390:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qca6390_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qca6390_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca9379:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca9379:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qca9379_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qca9379_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcn7605:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcn7605:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcn7605_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcn7605_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sc8180x:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sc8180x:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sc8180x_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sc8180x_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdx55:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdx55:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sdx55_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sdx55_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→