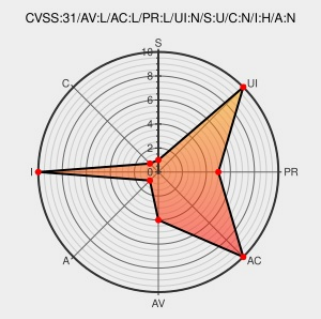
CVE-2019-14025

Published on: 09/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

CVE-2019-14025

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



Certain versions of Kamorta from Qualcomm contain the following vulnerability:

u'When a new session is created, Object is returned that contains TZ addresses and it get passed to HLOS as an handle to refer to a particular session and can cause TZ to jump to a invalid address' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130

CVE-2019-14025 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Qualcomm, Inc.** - **Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking** version **Kamorta, QCS404, QCS610, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
August 2020 Bulletin	Vendor Advisory www.qualcomm.com text/html	MISC www.qualcomm.com/company/product-security/bulletins/august-2020-security-bulletin
August 2020 Security Bulletin | Qualcomm	Broken Link www.qualcomm.com text/html	CONFIRM www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Qualcomm	Kamorta	-	All	All	All
Hardware	Qualcomm	Kamorta	-	All	All	All
Operating System	Qualcomm	Kamorta Firmware	-	All	All	All
Operating System	Qualcomm	Kamorta Firmware	-	All	All	All
Hardware	Qualcomm	Qcs404	-	All	All	All
Hardware	Qualcomm	Qcs404	-	All	All	All
Operating System	Qualcomm	Qcs404 Firmware	-	All	All	All
Operating System	Qualcomm	Qcs404 Firmware	-	All	All	All
Hardware	Qualcomm	Qcs610	-	All	All	All
Hardware	Qualcomm	Qcs610	-	All	All	All
Operating System	Qualcomm	Qcs610 Firmware	-	All	All	All
Operating System	Qualcomm	Qcs610 Firmware	-	All	All	All
Hardware	Qualcomm	Rennell	-	All	All	All
Hardware	Qualcomm	Rennell	-	All	All	All
Operating System	Qualcomm	Rennell Firmware	-	All	All	All
Operating System	Qualcomm	Rennell Firmware	-	All	All	All

Hardware	Qualcomm	Sc7180	-	All	All	All
Hardware	Qualcomm	Sc7180	-	All	All	All
Operating System	Qualcomm	Sc7180 Firmware	-	All	All	All
Operating System	Qualcomm	Sc7180 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
Hardware	Qualcomm	Sm6150	-	All	All	All
Hardware	Qualcomm	Sm6150	-	All	All	All
Operating System	Qualcomm	Sm6150 Firmware	-	All	All	All
Operating System	Qualcomm	Sm6150 Firmware	-	All	All	All
Hardware	Qualcomm	Sm7150	-	All	All	All
Hardware	Qualcomm	Sm7150	-	All	All	All
Operating System	Qualcomm	Sm7150 Firmware	-	All	All	All
Operating System	Qualcomm	Sm7150 Firmware	-	All	All	All
Hardware	Qualcomm	Sm8250	-	All	All	All
Hardware	Qualcomm	Sm8250	-	All	All	All
Operating System	Qualcomm	Sm8250 Firmware	-	All	All	All
Operating System	Qualcomm	Sm8250 Firmware	-	All	All	All
Hardware	Qualcomm	Sxr2130	-	All	All	All
Hardware	Qualcomm	Sxr2130	-	All	All	All
Operating System	Qualcomm	Sxr2130 Firmware	-	All	All	All
Operating System	Qualcomm	Sxr2130 Firmware	-	All	All	All

cpe:2.3:h:qualcomm:kamorta:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:kamorta:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:kamorta_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:kamorta_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcs404:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcs404:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcs404_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcs404_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcs610:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcs610:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcs610_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcs610_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:rennell:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:rennell:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:rennell_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:rennell_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sc7180:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sc7180:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sc7180_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sc7180_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:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sm6150:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sm6150:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sm6150_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sm6150_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sm7150:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sm7150:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sm7150_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sm7150_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sm8250:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sm8250:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sm8250_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sm8250_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sxr2130:-:*:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sxr2130:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sxr2130_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sxr2130_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→