# CVE Detail – CVE-2019-10482

Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.4569

## CVSS Scoring

CVSS v3.1 Score: 5.9

Severity: MEDIUM

## Affected Products

* cpe:2.3:o:qualcomm:apq8009\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:apq8017\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:apq8053\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:apq8096\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:apq8096au\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:apq8098\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9150\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9205\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9206\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9607\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9650\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8905\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8909\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8917\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8920\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8937\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8940\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8953\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8996\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8996au\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8998\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:nicobar\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qcs404\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qcs405\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qcs605\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qm215\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sa6155p\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sc8180x\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sda660\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sda845\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm429\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm439\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm450\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm630\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm632\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm636\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm660\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm670\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm710\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm845\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm850\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdx24\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdx55\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sm6150\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sm7150\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sm8150\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sm8250\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sxr1130\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sxr2130\_firmware:-:\*:\*:\*:\*:\*:\*:\*