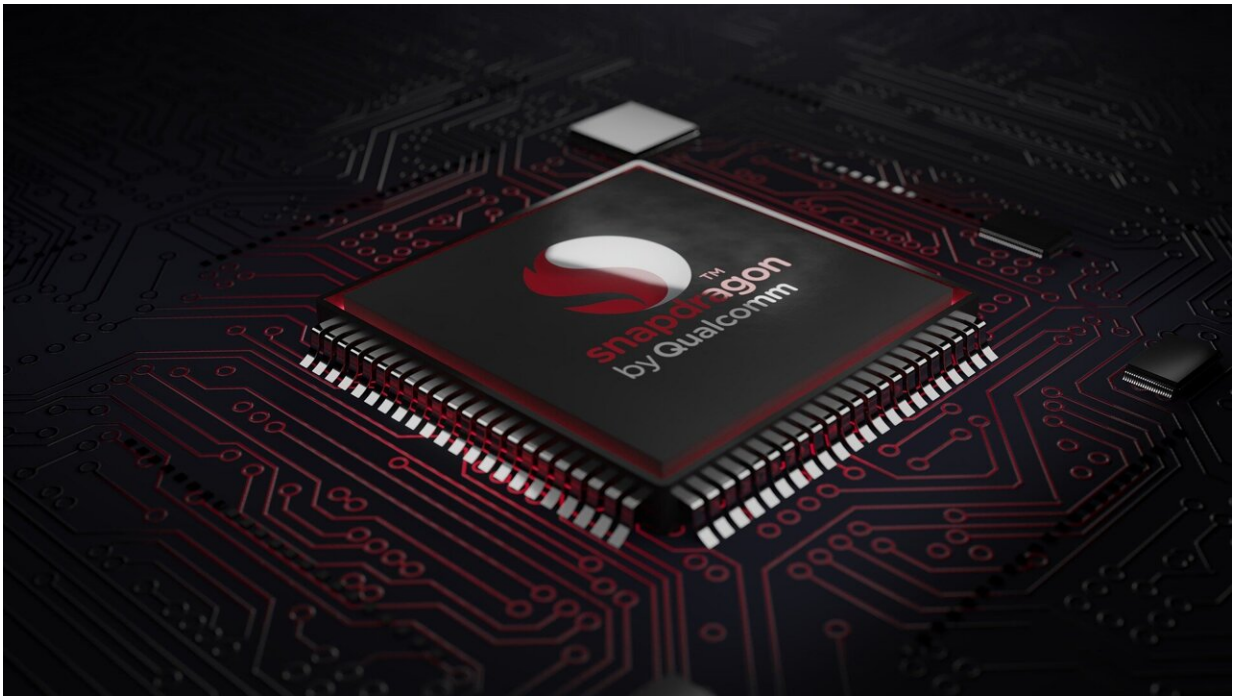
Check Point Research detects privacy flaw on Qualcomm's mobile station modems

May 7 2021, by Sarah Katz



Credit: Pixabay/CC0 Public Domain

Check Point Research (CPR) has identified a security flaw in the Qualcomm chip of the mobile station modems (MSM) used in cellular communication for over 40 percent of phones worldwide. If exploited, a hacker could use the vulnerability to infect Android OS with unseen, malicious code, thereby providing them access to user audio conversations as well as SMS threads and call history.

Indeed, many top-notch phone brands such as Android, LG, Samsung, One Plus and Xiaomi utilize MSM, meaning many phones stand to face impact from this flaw. Moreover, the vulnerability could even allow an attacker to access the phone's SIM card.

Such flaws present major risk to many users, as over three billion people globally use smartphones. In response to such a swiftly expanding market, many smartphone vendors have started depending on third-party manufacturers to produce both the hardware and software components of these devices.

Unfortunately, in 2020 alone, CPR has discovered over 400 security vulnerabilities on Qualcomm's Snapdragon DSP (Digital Signal Processor) chip, initially calling into question the usability of affected mobile phones. While this recent flaw appeared in MSM, the newer 5G is expected to expand to 1.9 billion subscriptions worldwide by the year 2024, meaning developers should be on the lookout for similar flaws in any upcoming versions.

Now, while over 30 percent of all mobile phones globally use MSM, researchers have yet to determine the amount of risk users of these devices face with regard to vulnerabilities of this nature.

However, security researchers were able to ascertain that an attacker desiring to break into the SIM card and access private conversations could simply exploit the MSM flaw via the 5G Qualcomm MSM Interface (QMI). Fortunately, researchers have also found that this flaw can be patched using the application processor.

The silver lining of this finding lies in the fact that researchers could now have an easier time investigating for such flaws in the modem code from within the modem itself, a feat which has commonly remained a significant obstacle for sanitizing and debugging.

Since its discovery, this flaw has been classified as CVE-2020-11292 and patched by Qualcomm, following notification to all impacted vendors.

In terms of users and organizations looking to safeguard their mobile devices, they should consider the following security best practices: Always keep the OS updated, only install applications downloaded from official app stores to avoid accidentally installing malware, enable remote wipe capability on all devices and implement a security solution for your mobile device.

More information: "Android Users' Privacy at Risk as Check Point Research Identifies Vulnerability on Qualcomm's Mobile Station Modems." Check Point Software, Check Point Software, 6 May 2021, blog.checkpoint.com/2021/05/06 … bile-station-modems/