SECURITY ADVISORY

Advisory Report on Qualcomm's "Achilles" vulnerabilities

CYBERPEACE

Date: 21/10/20

Summary: 400 hidden vulnerabilities have been found in Qualcomm's Digital Signal Processor.

Product: Qualcomm DSP.
Risk: Low to High

Over 400 hidden vulnerabilities have been found recently in Qualcomm's Hexagon Digital Signal Processor (DSP) which presents in almost all Snapdragon system-on-chip based mobile devices. Security solutions provider farm Checkpoint which is behind the exposure of the vulnerabilities has quoted the bugs as "Achilles". A wide number of chips provided by Qualcomm are embedded into the devices that count over 40% of the smartphone market which include the big brand phones like Samsung, Google, LG, Xiaomi, OnePlus as well as the others. Qualcomm has acknowledged the vulnerabilities and has also assigned them in six CVEs
"**CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208** and **CVE-2020-11209**."

What is DSP?

As the smartphone market is growing increasingly, the vendors are investing more on new features and capabilities. To support the technical innovations vendors often rely on third party solutions to provide compatible software's and hardware's. One of the most conventional solutions is Digital Signal Processor also known as DSP.

A DSP (Digital Signal Processor) is a system on a chip that has hardware and software designed to optimize and enable each area of use on the device itself, including:

- Charging abilities (such as “quick charge” features)
- Multimedia experiences e.g. video, HD Capture, advanced AR abilities
- Various Audio features

Simply put, a DSP is a complete computer on a single chip – and almost any modern phone includes at least one of these chips. A single SoC (Software on Chip) may include features to enable daily mobile usage such as image processing, computer vision, neural network-related calculations, camera streaming, audio and voice data.

Additionally, vendors can optionally use these “mini computers” to insert their own functionality that will run as dedicated applications on top of the existing framework.
The Digital Signal Processor developed by Qualcomm is known as Hexagon (QDSP6) which is designed as 4 way multi-threaded and belongs to the 32-bit microarchitecture family.

What is the Impact?

Though the DSP provides some solutions with more innovative features and functionalities, it comes with some vulnerabilities also. As mentioned above 40% of the mobile phones have embedded with Qualcomm’s DSPs, the number of the impacted users might be nearly 3 billion globally.
The number includes any Government Officials, people belonging to the industrial sector, nonprofit organizations as well as any people having the same chips embedded in their smartphones.

- The phones can be turned into spying instances without any intervention of the respective users.
- All the sensitive data including videos, images, realtime GPS data, microphone and call recording can be exfiltrated.
- Attackers can make the mobile phone unresponsive by rendering the data continuously and here comes the concept of Denial of Service attack.

- Hidden, undetectable malicious code can be injected remotely to the mobile device.

Though Qualcomm is going to release official patches for the vulnerabilities but one major issue with the android mobile devices is users continue to use the devices which are no longer being patched with latest security updates or OEMs.

Security Recommendations for Mobile users:

- Always update mobile devices with latest security patches as soon as it is available.

- Downloading apps from any third party (sideloading), unknown sources instead of the official app store should be avoided.

- Do not click any links coming from any untrusted source.

- Always use a paid reputed Antimalware solution.

- Always use a secured Wi-Fi network instead of getting connected to the internet through any unsecured public network.

- Data Encryption should be enabled.

- Always use Virtual Private Network (VPN) for sharing any confidential information.

- It is strictly unrecommended to jailbreak or get the root access of a mobile device.

References:

- https://blog.checkpoint.com/2020/08/06/achilles-small-chip-big-peril/
- https://www.bankinfosecurity.com/snapdragon-chip-flaw-could-facilitate-mass-android-spying-a-14802
- https://en.wikipedia.org/wiki/Qualcomm_Hexagon
- https://www.androidauthority.com/snapdragon-dsp-android-security-flaw-1146291/
- https://gadgets.ndtv.com/mobiles/news/qualcomm-compute-dsp-vulnerability-achilles-400-check-point-2276344

Revision Notes:

Version	Description	Section	Status	Date
1.0	Initial Public Release	---	Final	21/10/2020

Issued by
Research Wing, CyberPeace Foundation

www.cyberpeace.org
secretariat@cyberpeace.net

CYBERPEACE

/cyberpeacefoundation

/cyberpeacengo

/cyberpeacefoundation