New vulnerability on MediaTek chip makes 30% of Android smartphones can be eavesdropped

MediaTek has just had to immediately release patches for vulnerabilities that allow hackers to eavesdrop on Android users' calls. Even hackers can exploit the vulnerability to run commands or privilege escalation attacks.

MediaTek is one of the largest semiconductor companies in the world. As of the second quarter of 2021, MediaTek chips appear in 43% of all smartphones globally.

The vulnerabilities discovered by Check Point and three of them, CVE-2021-0661, CVE-2021-0662 and CVE-2021-0663 have been patched right in the October 2021 update MediaTek Security Bulletin. The fourth vulnerability, CVE-2021-0673, will be patched next month.

If you don't regularly install the latest security updates, newly discovered vulnerabilities on MediaTek chips will make Android smartphones vulnerable to eavesdropping attacks, malware infections or privilege escalation attacks.

Older smartphone models that no longer support security updates run the risk of not receiving MediaTek's patch.

Details of the vulnerability on the MediaTek chip

The new chipsets from MediaTek use a dedicated audio processor called Digital Signal Processor (DSP) to reduce CPU load and improve audio quality and performance.

The DSP receives audio processing requests from Android applications through the driver and the IPC system. Theoretically, an unprivileged application could exploit vulnerabilities to manipulate request processing and run

code on the DSP.

The audio driver does not communicate directly with the DPS, but with IPI messages that are passed to the System Control Processor (SCP).

By reversing the Android API code responsible for audio communication, Check Point discovered the following vulnerabilities:

1. CVE-2021-0661, CVE-2021-0662, and CVE-2021-0663: Incorrect bounds checks lead to out-of-bounds writes and local privilege escalation.
2. CVE-2021-0673: Details will be revealed next month.

By combining these vulnerabilities, hackers can perform local privilege escalation attacks, send messages to the DSP firmware, and hide or run code on the DSP chip itself.

"Since the DSP firmware has access to the audio data stream, a malformed IPI message can be exploited by a hacker to escalate privileges and theoretically could eavesdrop on smartphone users," Check Point said. To share.

Because there is no patch for the CVE-2021-0673 vulnerability, MediaTek has removed the ability to use the parameter string command through AudioManager to reduce the possibility of exploitation.

If you are using an Android smartphone equipped with a MediaTek chip, you should consider updating its software as soon as possible.