Detecting Qualcomm CPU errors can cause private data on the phone to leak

Security researchers have revealed a series of dangerous vulnerabilities that allow attackers to steal important personal information of smartphone owners running Qualcomm CPUs.

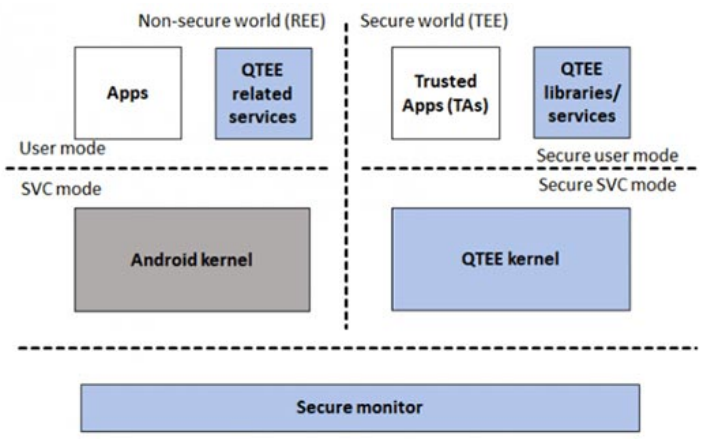
Security researchers from the Check Point Research team have revealed a series of dangerous vulnerabilities that appear on Qualcomm chipsets that allow attackers to steal important personal information of smartphone owners, along with a series of other risks related to rooting, unlocking bootloader and executing unknown APTs .

Qualcomm immediately confirmed the situation and worked with OEMs to issue patches in the form of system updates. Samsung and LG have applied patches to their devices, while Motorola is said to have fixed the problem.

Basically, Qualcomm CPUs often come with a secure area inside the processor called the Trusted Execution Environment (TEE). TEE's mission is to ensure the confidentiality and integrity of code and data based on ARM TrustZone technology - allowing the storage of the most sensitive data without risk of tampering.

In addition, this 'security world' provides some additional services in the form of trusted third-party components (also known as trustlets) that are loaded and executed in TEE by the operating system running in TrustZone - called the trusted OS (trusted OS).

Trustlets will act as a bridge between the 'normal' world - the rich execution environment where the device's main operating system (e.g. Android) exists - and the TEE, thereby enabling Move data between two 'worlds'.



TrustZone will be a place for important data such as passwords, credit card information for mobile payments, encryption keys and more. Thus, if a hacker invades this area through a vulnerability, nothing will prevent your

sensitive data from being stolen.

Qualcomm said that without access to the hardware keys of the device, you would not be able to access data stored in QTEE unless there was a flaw in which the keys were exposed. And this is exactly the problem that Qualcomm chipset is having.

To find this flaw, Check Point researchers used a technique called fuzzing - an automated testing method that involves providing random data as input to a computer program to causing it to crash, thereby identifying undesirable programming behaviors and errors that can be exploited to provide corrective measures.

According to research results, vulnerabilities on Qualcomm CPUs could allow an attacker to execute applications in the 'normal world', load an application into a 'security world' and even load trustlets from another device.

There have not been any actual attacks recorded, the prospects for crooks to exploit these holes are huge. Attacks on TrustZone are a way to gain access to protected data on mobile devices. And such an attack will be used as part of an exploit chain starting from installing a malicious application to a device or spreading through a malicious link.