Phones from 11 manufacturers may be attacked by hidden AT commands

Researchers have found that millions of mobile devices come from 11 smartphone manufacturers that can be attacked by AT commands.

Researchers have found that millions of mobile devices come from 11 smartphone manufacturers that can be attacked by AT commands.

The AT (ATention) or Hayes script, which consists of short string commands, has been developed since the early 1980s for transmission over telephone lines and modem control.Different AT commands can be combined to tell the modem to call, hold or change connection parameters.

A team of researchers from the University of Florida, Stony Brook and Samsung Research America have found out which AT command is currently supported on Android devices.Analysis of more than 2,000 Android firmware from 11 OEMs such as ASUS, Google, HTC, Huawei, Lenovo, LG, LineageOS, Motorola, Samsung, Sony and ZTE, they found that these devices support more than 3,500 AT command types, some of them have potential risks.

These AT commands are likely to be attacked via USB interface, when an attacker takes over the device or hides malicious code inside the dock or charging station.When connected, an attacker can use the secret AT command to rewrite the device's firmware, bypass Android's security mechanism, get important information .

In the best case, AT commands will only work when USB Debugging is turned on, but on many devices, the attacker can directly access the AT command even though the device is locked.Sometimes OEMs do not mention these commands.

Below is a video describing the actual attack on LG G4

As the video above, the most dangerous is when an attacker can mimic the touch screen, take full control of the device, install a malicious application to continue monitoring.

Phone manufacturers have been notified of the AT attack capability via the phone's USB interface.They also posted a website of phone models and a firmware version that could be hacked.

After checking the AT commands on the Android device via USB interface, researchers will also work on Apple devices, but only if the AT command can be used via remote access connections such as WiFi. or Bluetooth.

Site list of devices and firmware *https://atcommands.org/atdb/vendors*

See more:

1. Fortnite for Android has a security vulnerability
2. Android collects user data even when the device is not 50 times more than iOS
3. 5 types of malware on Android

You finished reading the article "**Phones from 11 manufacturers may be attacked by hidden AT commands**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
