

Apple: Security flaw in iPhone's USB-C port is not a concern

New security vulnerability discovered on USB-C controller of iPhone 15 and 16, should users worry?

Despite the convenience it brings to users, the USB-C port on the new iPhone also poses security risks. Recently, researcher Thomas Roth discovered several vulnerabilities in the USB-C controller of the iPhone 15 and 16, allowing hackers to access the firmware and execute malicious code. However, Apple said that these attack methods are still complicated and users do not need to worry yet.



The USB-C port on new iPhones has a security flaw.

Roth demonstrated the technique of "dumping" the firmware of a USB-C controller at the 38th Chaos Communication Congress. This helps hackers analyze source code, find vulnerabilities, and develop malware.

While Apple has not made any moves yet, it is possible that the company will have to update the hardware for future iPhone models such as the iPhone SE 4 and iPhone 17 to patch the security holes.

The move to USB-C on iPhones is partly due to new European Union regulations. However, the standard also brings new security challenges for Apple. In addition, poor quality USB-C cables on the market can also contain hidden hardware circuits that can be used to spread malware or steal data.

However, there are some benefits to dumping your firmware. It helps independent repair professionals better understand your Mac's hardware, making it easier for you to fix your device.

You finished reading the article "**Apple: Security flaw in iPhone's USB-C port is not a concern**" 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.