WiFi error when connecting to a special network name that can be used to hack iPhone

Security researchers say the bug that crashes WiFi service on iPhones can be exploited to execute malicious code remotely without user interaction.

Initially, this bug can disable the iPhone's WiFi connection when connecting to a network whose name (SSID) includes a special character. However, not only that, this bug can also be exploited to hack into iPhone.

Researchers from the startup ZecOps have discovered that based on a WiFi connection error on iPhones, it can be exploited to execute malicious code remotely without user interaction. They named this type of attack WiFiDemon.

While trying to exploit the vulnerability, ZecOps tried adding the SSID name "%@", a format for printing and formatting objects in Objective-C, the programming language for iOS software.

According to ZecOps, if they find an object released on the stack, they can use injection to control the contents of that memory. Next, they use "%@" to treat it like an Objective-C, such as a typical Use-After-Free that could lead to remote code execution.

The researchers succeeded by simply adding "%@" to the SSID. One scenario that can lead to remote execution of malicious code on the target device is to create a malicious WiFi network and wait for the victim to connect.

On previous iOS versions, even the victim does not connect to WiFi containing malicious code, the WiFi service also crashes and restarts continuously right after reading the SSID is intentionally misspelled. If the bug is exploited locally, an attacker can create a temporary sandbox to jailbreak the device.

ZecOps shared that they found no evidence that WiFiDemon was exploited by hackers. However, it is not excluded that cybercriminals already know about this vulnerability and are looking to exploit it.

WiFiDemon is especially dangerous on iOS 14 to iOS 14.4 because it does not require user interaction. However, Apple released an update to fix the problem in January 2021.

In its safety recommendation, ZecOps recommends that users update their iPhones to the latest iOS version. In addition, users should turn off the automatic WiFi connection feature.

As expected, the iOS 14.7 update that Apple recently released will fix the problems reported by ZecOps. However, in the iOS 14.7 update information, Apple does not mention this issue.

You finished reading the article "**WiFi error when connecting to a special network name that can be used to hack iPhone**" 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.

© 2019 TipsMake.com