Many serious vulnerabilities have been discovered that allow attackers to take full control of the 4G router

In the past few months, security experts around the world have found that many vulnerabilities exist in 4G routers.

In the past few months, security experts around the world have found that many vulnerabilities exist in 4G routers from a number of well-known production and market share. school In particular, most of these vulnerabilities will cause users to leak information, and create conditions for those who deploy remote execution commands.

In a recent discovery related to security holes in 4G routers, cyber security researchers nicknamed 'G Richter' from security organization Pen Test Partners shared information about a series of losses. The simple to complex vulnerabilities that he and his colleagues found on 4G router devices, in the framework of the 2019 global DEF CON security conference have just taken place in Las Vegas this year, and confirmed that "a lot of modems and 4G routers currently used worldwide are unsafe".

1. Discover new ways to hack WPA3 protected WiFi passwords

Routers are generally one of the network devices often targeted by hackers

'My colleagues and I have found some serious vulnerabilities that appear on 4G routers from different manufacturers. These holes can be trusted by remote exploitation through a number of quick and uncomplicated exploits, 'said Richter.

Also according to experts, only a small group of network hardware equipment manufacturers are now working really seriously and showing interest in mobile security and hardware technologies (also as software dependency).

Not stopping there, what's worse is that security vulnerabilities have been found appearing on a large number of network devices from every price segment, from routers and dongles to high-end users to Extremely expensive devices, which are designed for use in large enterprise networks . all contain security holes that allow hackers to take control of the device and infiltrate the network.

Let's take a look at some of the vulnerabilities discovered in 4G router products from major manufacturers, taking a significant share of the market.

1. Two 9th graders attacked the school's wifi network so they wouldn't have to take a test

Security vulnerabilities in ZTE routers

Until now, ZTE has always been a network equipment manufacturer to create a very good impression in the eyes of the international security community with enthusiasm and dedication to overcome the reported vulnerabilities. For example, the case of the two models MF910 and MF65 +, although discovered to contain a vulnerability at the end of the support period, but ZTE still quickly released patches for users, this is very commendable. .

However, the fact that ZTE's products are frequently found to contain security holes has also affected the reputation of this Chinese manufacturer. This time with the MF920 router model, which uses the same code base with its predecessor, the measurement also contains nearly the same vulnerabilities. ZTE is committed to fixing the reported bugs (being tracked through CVE identifiers).

1. Most mobile calls in the world today can be eavesdropped by hackers

ZTE MF920 4G router

Here are some issues discovered by G Richter's team while testing two MF910 and MF65 router models, which have not been patched by ZTE yet:

1. Administrator password may be leaked (authenticated first).
2. One of the debugging endpoints can easily be command injection attacks.
3. There is the presence of a Cross-Site Scripting point.

These problems can be 'connected' to allow arbitrary execution of malicious code on the router, after the user accesses the attacker's malicious website.

For the MF920 router, there were two vulnerabilities found and monitored as follows:

1. CVE-2019-3411 - Information leakage (CVSS v3.0 basic point: 7.5, high severity)
2. CVE-2019-3412 - Execute arbitrary command (CVSS v3.0 point: 9.8, extremely serious risk level)

Security errors found in Netgear and TP-LINK 4G routers

The Pen Test Partners team also found security issues in some 4G routers manufactured by Netgear and TP-LINK, with at least 4 of them also being assigned CVE identifiers for easy tracking.

In the case of the NETGEAR Nighthawk M1 Mobile router, the vulnerability bypasses cross-site request requests that are tracked with CVE-2019-14526), ??and command injection after authentication (CVE-2019-14527) may allow an attacker to potentially execute arbitrary code on the device, especially in the case where "the user places a password on the web interface not strong enough".

1. Alarming statistics on the situation of network security in our country in the first half of 2019

4G Netgear Nighthawk M1 Mobile Router

This security flaw can easily be exploited by an attacker by tricking users into accessing a malicious page created by themselves.

Besides, another popular model currently used is the TP-LINK M7350 4G LTE Mobile wireless router that has been found to contain vulnerable vulnerabilities, this time with command injection errors that are tracked with intentions. the following list:

1. CVE-2019-12103 - Execute the command before authentication
2. CVE-2019-12104 - Execute the command after authentication

4G TP-LINK M7350 4G LTE Mobile Router

Due to work requirements, more and more people choose to use 4G routers instead of traditional network data receivers / transmitters. Therefore, the security holes hidden in these products, if not timely overcome, will make more and more people at risk of becoming victims of hackers.

In addition to trying to launch new products, manufacturers should also pay more attention to the release of patches for the reported vulnerabilities on their products.