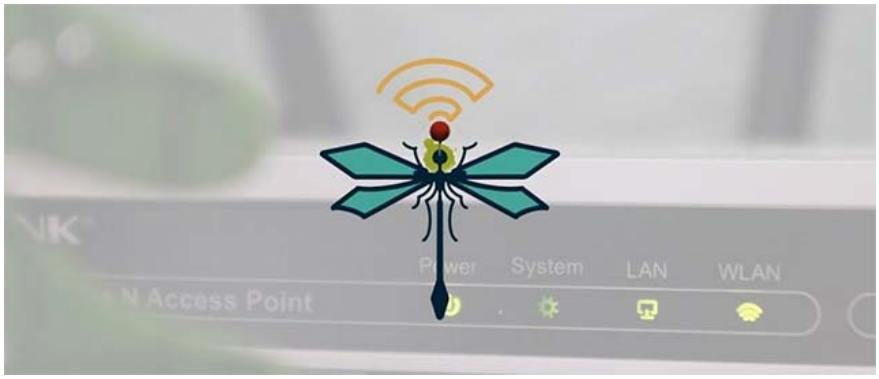
Discover new ways to hack WPA3 protected WiFi passwords

Earlier this month, it was the cyber security team that found Dragonblood to continue to release two more serious vulnerabilities that could allow an attacker to easily hack the target WiFi password.

Four months ago, a group of network security researchers from Tel Aviv University and KU Leuven discovered some serious security holes, collectively called Dragonblood, hidden in WiFi security standards. WPA3, which allows potential attackers to unlock Wi-Fi network passwords, and thereby gain access to encrypted network traffic, being exchanged between connected devices.

Earlier this month, the same network security researcher continued to release two more serious vulnerabilities that could allow an attacker to easily hack the target WiFi password.

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



Dragonblood is a dangerous security vulnerability discovered in WPA3

WPA (short for WiFi Protected Access) is a WiFi security standard, designed to authenticate wireless devices with AES (Advanced Encoding Standard) protocol and aims to prevent hackers from accessing data your rope.

Basically, WPA3 uses the Wi-Fi Device Provisioning Protocol (DPP) protocol instead of the shared password to log new devices into the network. This is a protocol that allows users to scan QR or NFC codes to log devices into the wireless network, replacing the traditional password usage method. In addition, unlike WPA2, all network traffic on WPA3 will be encrypted after connecting to a network system using WPA3 WiFi Security.

The WiFi Protected Access III (WPA3) protocol was released more than a year ago as an alternative to WPA2 - an 'aging' protocol that is 14 years old and is currently showing less safety. WPA3 is expected to solve the technical shortcomings of the WPA2 protocol from the basics. These disadvantages have long been considered unsafe and easily caused the WiFi connection to be attacked by KRACK at a more serious level.

WPA3 secures WiFi connectivity through a more secure 'steel shield', called concurrent authentication (Authentication of Equals - SAE). SAE is also known as Dragonfly, which gives WiFi networks the ability to protect against attacks with stronger password-based authentication methods.

1. Detecting vulnerabilities in Snapdragon chips allows hackers to penetrate nearly every Android smartphone via wifi

WiFi Protected Access III (WPA3)

However, in less than a year, two security researchers Mathy Vanhoef and Eyal Ronen (Tel Aviv & KU Leuven University) found some weaknesses (Dragonblood) when deploying WPA3, allowing attackers to Find out the WiFi password by abusing the time or buffer-based channel leakage (cache-based side-channel leak).

Shortly after the flaw was revealed, the WiFi Alliance, a non-profit organization that oversees the application of the global WiFi standard, immediately released patches to solve the problem, and at the same time released Security recommendations to minimize Dragonblood attacks.

But after a few months of implementation, the fact has shown that these security recommendations - created by the internal WiFi Alliance without any cooperation with free security researchers - are not strong enough. to protect users against Dragonblood attacks.

Not only that, it also 'paved the way' for two new side-channel attacks, again allowing an attacker to steal a user's WiFi password even when they are using a session. Latest WiFi security protocol.

1. This is why you should plug in the network cable when playing games instead of using wifi

New side channel attacks target WPA3 when using Brainpool Curve

The first flaw, tracked under the CVE-2019-13377 identifier, is a time-based side-channel attack against WPA3's Dragonfly authentication method using Brainpool curves. Ironically, this is the channel the WiFi Alliance recommends that suppliers should use to add another layer of security against previous Dragonblood attacks.

The analysis table of the Dragonfly WPA3 vulnerability of Mathy Vanhoef and Eyal Ronen

The researchers found that using Brainpool Curve unintentionally opened a second-party channel leak in WPA3's Dragonfly authentication method. In other words, even if users fully comply with the security recommendations of WiFi Alliance, their WiFi connection is still at risk of being attacked.

"New side channel leak is in Dragonfly's password encryption algorithm. We have confirmed the new Brainpool leak in practice regarding the latest Hostapd version, and you can brute-force the password by using leaked information, 'the team said.

1. Using an outdated network driver, the computer may lose WiFi connection after installing Windows 10 May 2019 Update

Side channel attack targets EAP-PWD of FreeRADIUS

The second flaw, followed by the identifier CVE-2019-13456, is an information leak that stems from the deployment of EAP-pwd (Password Extension Authentication Protocol) in FreeRADIUS, one of the machines The world's most widely used open source RADIUS host. In fact, RADIUS is often used by organizations and businesses as a central database to authenticate remote users.

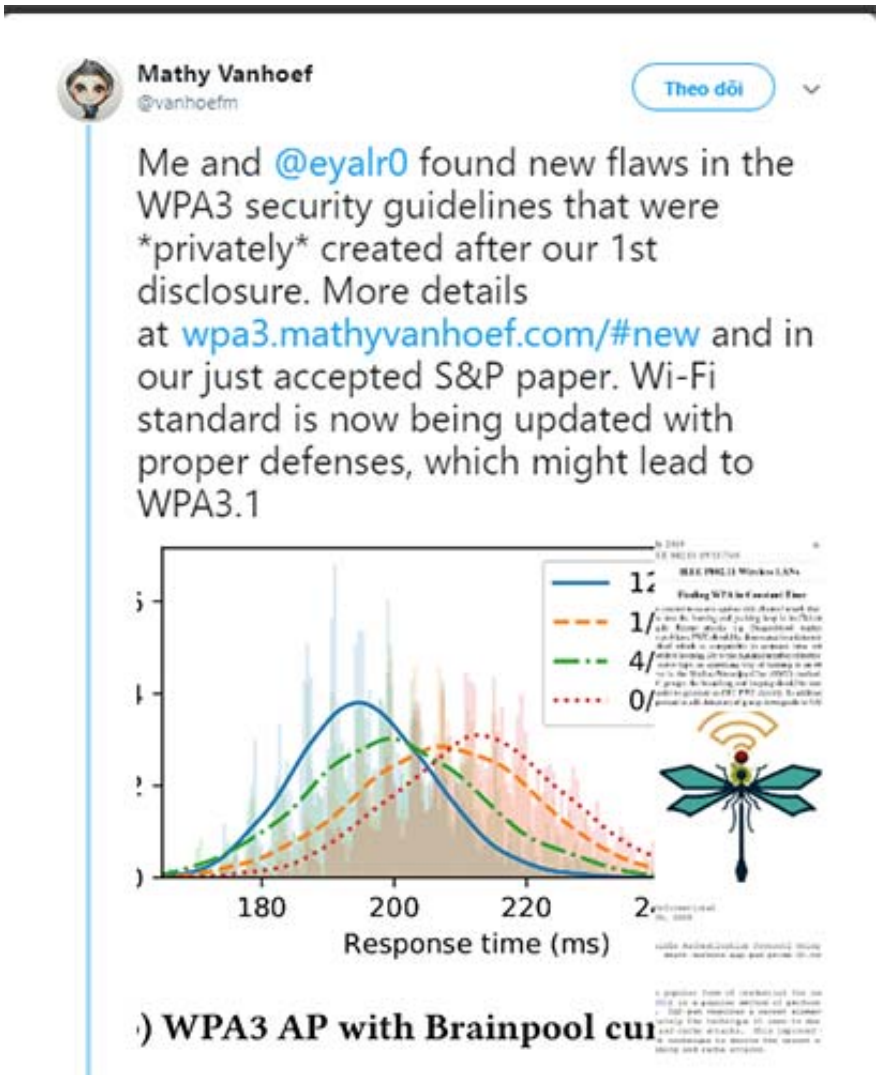
Math Vanhoef, one of the two researchers, discovered the Dragonblood vulnerability, saying that an attacker could completely target EAP-pwd to find and leak information, then this information could Used to recover a user's WiFi password by performing brute-force attack.

"The EAP-pwd protocol uses Dragonfly internally, and this protocol is also deployed in some enterprise network systems, where users often authenticate with usernames and passwords. More worrisome, We found that the WiFi firmware of Cypress chip only performed at least 8 repetitions to prevent side channel leaks, although this made the deployment of attacks more difficult, but could not prevent Block them completely, "the team said.

Also, according to the researchers, deploying Dragonfly and WPA3 algorithms without causing side channel leaks is an extremely difficult and almost impossible task. At the same time, backward compatible countermeasures with these attacks often exceed the capabilities of conventional devices.

Mathy Vanhoef and Eyal Ronen shared their new findings with the WiFi Alliance and posted on Twitter: "The WiFi standard is currently being updated with appropriate defense measures, which can lead to WPA 3.1", Unfortunately, new defense measures are not compatible with the original version of WPA3.

1. What is the purpose of Google providing free wifi in Vietnam? Is there really a 'free meal'?



"WiFi standards are currently being updated with appropriate defense measures, which can lead to WPA 3.1"

In the latest move, security expert Mathy Vanhoef said in an interview that the WiFi Alliance created their privacy principles in private mode, and this is a way that is not appreciated. "If only they had done this publicly, the problems that we'd found out were completely unavoidable. Even the original WPA3 certification was done privately, this wasn't It doesn't make sense. "

You finished reading the article "**Discover new ways to hack WPA3 protected WiFi passwords**" 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.