

What is WPA2 (WiFi Protected Access 2)?

WPA2 stands for WiFi Protected Access 2, WPA2 is a security method added to WPA for wireless networks, to provide stronger data protection and network access control capabilities.

WPA2 provides business and home WiFi users with a high degree of assurance that only authorized users can access their wireless network.

Based on the IEEE 802.11i standard, WPA2 provides government-grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm FIPS 140-2, same 802.1x-based authentication.



There are two versions of WPA2: WPA2-Personal and WPA2-Enterprise:

1. WPA2-Personal protects against unauthorized network access using a set password.
2. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

Vulnerability discovered in WPA2 . protocol

On October 16, 2017, security researchers disclosed a high-severity vulnerability in the WPA2 protocol, making it possible for attackers to eavesdrop on WiFi traffic passing between computers and other devices. access point.



The Proof-Of-Concept exploit attack known as KRACK (Key Reinstallation Attacks) affects the core WPA2 protocol itself and is effective against devices running Android, Linux, Apple, Windows and OpenBSD operating systems, as well as MediaTek Linksys and many other types of operating systems running on the devices. Vendors then provided patches and updates to users to fix this vulnerability.

You finished reading the article "**What is WPA2 (WiFi Protected Access 2)?**" 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.