WPA3 Network Password Bypassed via MITM Attack & Social Engineering

Researchers have successfully bypassed the Wi-Fi Protected Access 3 (WPA3) protocol to obtain network passwords using a combination of Man-in-the-Middle attacks and social engineering techniques.
The research, conducted by Kyle Chadee, Wayne Goodridge, and Koffka Khan from the University of the West Indies, highlights potential vulnerabilities in the latest wireless security standard.

WPA3, introduced in 2018, was designed to address the shortcomings of its predecessor, WPA2, and provide enhanced security for Wi-Fi networks. One of its key features is the Simultaneous Authentication of Equals (SAE) protocol, which was intended to make passwords resistant to offline dictionary attacks.

However, the researchers demonstrated that it is possible to exploit weaknesses in WPA3s transition mode, which allows for backwards compatibility with WPA2 devices.

By leveraging a downgrade attack, they were able to capture part of the WPA3 handshake, which was then used in conjunction with a social engineering technique to recover the network password.

The attack methodology consisted of three main steps:

Capturing the handshake using a downgrade attack
Deauthenticating users from the original WPA3 network
Spawning an evil twin access point with a captive portal to obtain the password
The researchers used a Raspberry Pi to simulate a WPA3 access point and employed open-source tools such as Airgeddon to create the rogue access point and captive portal.

When unsuspecting users attempted to connect to the fake network, they were prompted to enter the Wi-Fi password, which was then verified against the captured handshake.

This research raises concerns about the security of WPA3, particularly in its transition mode. The study found that the attack was successful when Protected Management Frames were not implemented, a setting that many users may not be aware of or have enabled.

Interestingly, the researchers also discovered that some devices were unable to connect to WPA3 transition networks, contradicting claims by the Wi-Fi Alliance about backward compatibility with WPA2.

While the attack requires specific conditions and user interaction, it demonstrates the ongoing challenges in securing wireless networks. The researchers emphasize the importance of user education and proper configuration of WPA3 networks to mitigate such risks.

Cybersecurity experts are calling for further investigation into WPA3s vulnerabilities and the development of additional safeguards. As Wi-Fi networks continue to be critical infrastructure for businesses and individuals alike, ensuring their security remains paramount.

The findings of this study serve as a reminder that even the most advanced security protocols can be susceptible to clever combinations of technical exploits and social engineering.

As WPA3 adoption increases, it is crucial for both users and manufacturers to remain vigilant and implement best practices to protect wireless networks from potential attacks.

The research team plans to continue their work, exploring additional vulnerabilities and developing countermeasures to enhance the security of WPA3 and future wireless protocols.

Their efforts contribute to the ongoing battle between cybersecurity professionals and potential attackers in the ever-evolving landscape of digital security.

Quelle: Cyber Security Monitor Worldwide vom 24.12.2024

Ressort:	Cyber Security
Dokumentnummer:	465928663