American
Technology Services

2017-06 ATS Security Advisory

WPA Protocol Vulnerability (KRACKs)

Summary

On Monday, October 16th, 10 new vulnerabilities were announced which affect WPA 1 and 2, with both PSK and Enterprise configurations. These vulnerabilities may allow an attacker to view data transmitted between a client and an access point (AP) which were previously assumed to be encrypted. This vulnerability is considered critical, because it affects a standard security protocol that is widely implemented by various vendors in wireless networking hardware worldwide. However, successful exploitation of these vulnerabilities is difficult due to various factors. For example:

- A successful attack requires physical proximity to a victim's wireless network.
- Other, widely used security protocols (such as TLS) may mitigate an attempted attack.
- Some current implementations of WPA may not be exploitable.

Details

The researchers who discovered this vulnerability have called the attack a "**k**ey **r**einstallation **a**tta**ck"** (KRACKs). Their method attacks part of the 4-way handshake that takes place when a client connects to a wireless access point (AP). In order to maintain sufficient randomness when communicating using WPA2, the AP and client agree on an initialization vector, or "nonce," which is a number that is incremented and included with subsequent messages. The key and the nonce form a "keystream" that is used to encrypt data. For WPA2 to maintain security, the keystream must only be used once. Researchers discovered that by replaying parts of the handshake, the AP can be forced to reset the nonce back to its initial state. This causes the keystream to be reused. Keystream reuse allows more sophisticated cryptographic attacks which can allow an attacker to replay, decrypt, or forge communication.

Risk Mitigation Steps Taken by ATS on Behalf of Customers

Vendors of affected hardware were made aware of this weakness before today’s general release. Vendors are taking steps individually to address the risks presented to their specific products. ATS is keeping a close eye on vendor guidance and implementing patches and other steps for mitigation as new information is released.

An updated list of vendor responses can be found here: https://github.com/kristate/krackinfo

Future Risk Mitigation

This was the first weakness reported against the WPA2 protocol. As vendors release updates to address these vulnerabilities the risk of being affected will decrease. We do not expect this to have a lasting impact on wireless networks or the WPA2 protocol as a whole. This weakness does highlight the importance of keeping both client and infrastructure hardware (such as APs) up to date with current firmware, patches, etc.

Understanding current threats and the security posture of your organization is important and ATS can help by providing a Vulnerability Assessment and Penetration Test (VAPT). For more information, reach out to your ATS Account Manager or send an email to security@networkats.com.

What Can You Do?

The worst-case scenario with this weakness is that you are connected to an essentially untrusted wireless network, as if you were at a Starbucks or an airport. Encrypted connections still cannot be viewed in these scenarios: Always ensure you are connected to websites over HTTPS. Ensure other services are using similar encrypted protocols such as SSH and SFTP.

Keep an eye out for communication from wireless hardware vendors you use to connect to wireless networks (phones, laptops, etc.) Apply updates as they become available to ensure you are protected from this vulnerability. Be aware that this is an opportune time for phishers to take advantage of the heightened security concern. Official emails should always come directly from your vendor and links should point to their official domain (cisco.com, for example).

Feel free to contact security@networkats.com with any questions or concerns. As always, we value hearing from our clients about general and specific security concerns so that we can provide the best possible services.