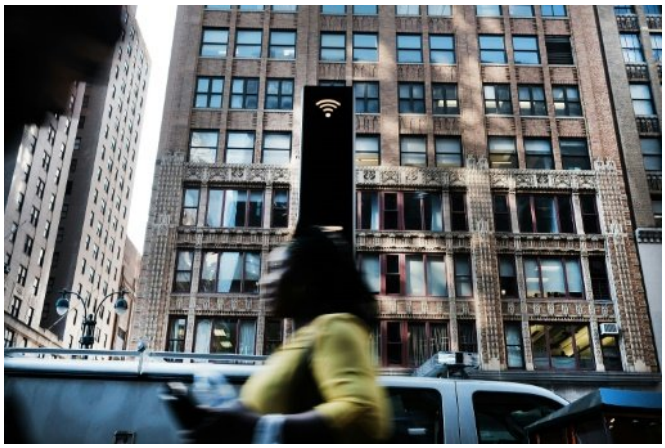
US warns of security flaw which can compromise Wi-Fi connections (Update)

16 October 2017



Security researchers have discovered a flaw which can compromise the security of Wi-Fi connections, according to a US government warning

A newly discovered flaw in the widely used Wi-Fi encryption protocol could leave millions of users vulnerable to attacks, prompting warnings Monday from the US government and security researchers worldwide.

The US government's Computer Emergency Response Team (CERT) issued a security bulletin saying the flaw can open the door to hackers seeking to eavesdrop on or hijack devices using wireless networks.

"Exploitation of these vulnerabilities could allow an attacker to take control of an affected system," said CERT, which is part of the US Department of Homeland Security.

The agency's warning came on the heels of research by computer scientists at the Belgian university KU Leuven, who dubbed the flaw KRACK, for Key Reinstallation Attack.

According to the news site Ars Technica, the discovery was a closely guarded secret for weeks to allow Wi-Fi systems to develop security patches.

Attackers can exploit the flaw in WPA2—the name for the encryption protocol—"to read information that was previously assumed to be safely encrypted," said a blog post by KU Leuven researcher Mathy Vanhoef.

"This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected Wi-Fi networks."

The researcher said the flaw may also allow an attacker "to inject ransomware or other malware into websites."

The KRACK vulnerability allows attackers to circumvent the "key" on a Wi-Fi connection that keeps data private.

The Belgian researchers said in a paper that devices on all operating systems may be vulnerable to KRACK, including 41 percent of Android devices.

'Be afraid'

The newly discovered flaw was serious because of the ubiquity of Wi-Fi and the difficulty in patching millions of wireless systems, according to researchers.

"Wow. Everyone needs to be afraid," said Rob Graham of Errata Security in a blog post.

"It means in practice, attackers can decrypt a lot of Wi-Fi traffic, with varying levels of difficulty depending on your precise network setup."

Alex Hudson, of the British-based digital service firm Iron Group, said the discovery means that "security built into Wi-Fi is likely ineffective, and we should not assume it provides any security."

Hudson said Wi-Fi users who browse the internet should still be safe due to encryption on most websites but that the flaw could affect a number of internet-connected devices.

"Almost certainly there are other problems that will come up, especially privacy issues with cheaper Internet-enabled devices that have poor security," Hudson said in a blog post.

Researchers at Finland-based security firm F-Secure said in a statement the discovery highlights longstanding concerns about Wi-Fi systems' vulnerability.

"The worst part of it is that it's an issue with Wi-Fi protocols, which means it affects practically every single person in the world that uses Wi-Fi networks," F-Secure said in a statement.

The F-Secure researchers said wireless network users can minimize the risks by using virtual private networks, and by updating devices including routers.

The Wi-Fi Alliance, an industry group which sets standards for wireless connections, said computer users should not panic.

"There is no evidence that the vulnerability has been exploited maliciously, and Wi-Fi Alliance has taken immediate steps to ensure users can continue to count on Wi-Fi to deliver strong security protections," the group said in a statement.

"Wi-Fi Alliance now requires testing for this vulnerability within our global certification lab network and has provided a vulnerability detection tool for use by any Wi-Fi Alliance member."

Microsoft said it released a patch on October 10 to protect users of Windows devices.

"Customers who have Windows Update enabled and applied the security updates, are protected automatically," Microsoft said.

A Google spokesman said, "We're aware of the issue, and we will be patching any affected devices in the coming weeks."

More information: www.krackattacks.com/