Crossing the Digital Divide (v86)

“There’s more”

By Joseph Feigon

For the Observer

This week’s article is more technical than most, but the message is simply stressing the importance of routine backups and software patching.

Microsoft Windows runs on most home computers, and no version has escaped software errors, many of which have or could have crippled computer operations for the user/owner. Consistent attention to software and firmware updates, including any applications (Office, Adobe, Quickbooks, Malwarebytes, etc.), will ensure you years of safe surfing, but what of the other elements in your network? Yes, that wireless router you’ve been so dependent upon needs updating too, and today is a good time to do so.

WPA/WPA2, the latest “standard” for wireless encryption has been found to contain software errors that could easily lead to a compromised network. It’s yours, not theirs, so let’s log onto those routers and wireless access points and update firmware. Netgear, Cisco, Ubiquiti, Asus and more, the coding errors are common, fortunately, so is the patch, provided you download and install it!

Overview

Wi-Fi Protected Access (WPA, more commonly WPA2) handshake traffic can be manipulated to induce nonce and session key reuse, resulting in key reinstallation by a wireless access point (AP) or client. An attacker within range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocols being used. Attacks may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast and group-addressed frames. These vulnerabilities are referred to as Key Reinstallation Attacks or "KRACK" attacks.

Description

Reusing a Nonce, Key Pair in Encryption

Wi-Fi Protected Access II (WPA2) handshake traffic can be manipulated to induce nonce and session key reuse, resulting in key reinstallation by a victim wireless access point (AP) or client. After establishing a man-in-the-middle position between an AP and client, an attacker can selectively manipulate the timing and transmission of messages in the WPA2 Four-way, Group Key, Fast Basic Service Set (BSS) Transition, PeerKey, Tunneled Direct-Link Setup (TDLS) PeerKey (TPK), or Wireless Network Management (WNM) Sleep Mode handshakes, resulting in out-of-sequence reception or retransmission of messages. Depending on the data confidentiality protocols in use (e.g. TKIP, CCMP, and GCMP) and situational factors, the effect of these manipulations is to reset nonces and replay counters and ultimately to reinstall session keys. Key reuse facilitates arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast, broadcast, and multicast frames.

Impact

An attacker within the wireless communications range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocol being used. Impacts may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast, broadcast, and multicast frames.

Solution

Install Updates

The WPA2 protocol is ubiquitous in wireless networking. The vulnerabilities described here are in the standard itself as opposed to individual implementations thereof; as such, any correct implementation is likely affected. Users are encouraged to install updates to affected products and hosts as they are available. For information about a specific vendor or product, check the Vendor Information section of this document or contact the vendor directly. Note that the vendor list below is not exhaustive.

Control those things you can, and keep the surprises to a minimum!