Fluke Networks Releases New Signatures to Protect Against WLAN Vulnerabilities

Fluke Networks released new threat signatures for its AirMagnet Enterprise 9.0 wireless intrusion detection and prevention system (WIDS/WIPS), including a signature for the recently discovered Wi-Fi Protected Setup (WPS) PIN Brute Force attack. The update also includes threat signatures to protect against Domain Name Server (DNS) and Internet Control Message Protocol (ICMP) Tunneled Traffic, and 802.11 Fuzzing attacks.

The new signatures protect against four attacks that can exploit wireless LANs (WLANs):

• Wi-Fi Protected Setup PIN Brute Force Attack – Wi-Fi Protected Setup (WPS) is a simplified method for configuring security settings that is supported on certain access points and clients. On Dec. 27, 2011, a serious vulnerability was reported in the WPS mechanism that allows an attacker to derive the PIN and therefore gain unauthorized connection to the access point (AP). There are currently two known attack tools that exploit this vulnerability.

• DNS Tunneled Traffic Detection – Domain Name Server (DNS) tunneling is the practice of encapsulating TCP traffic inside DNS packets. This technique can be used to bypass payment and gain unauthorized connectivity through Wi-Fi Hotspots or other protected guest access portals.

• ICMP Tunneled Traffic Detection – Similar to the DNS Tunneling Traffic Detection, Internet Control Message Protocol (ICMP) tunneling is the practice of encapsulating Transmission Control Protocol (TCP) traffic inside ICMP packets. This technique can also be used to bypass payment and gain unauthorized connectivity through Wi-Fi Hotspots or other protected guest access portals.

• 802.11 Fuzzing Attack – 802.11 Fuzzing is the process of introducing invalid, unexpected or random data into 802.11 frames and then replaying those modified frames into the air. This can cause unexpected damage to the destination device including driver crashes, operating system crashes and stack-based overflows that would allow execution of arbitrary code on the affected system, including APs.

AirMagnet Enterprise is the only WLAN security system that can immediately generate signature updates for immediate protection against new threats and automatically push them to customers without requiring scheduled downtime or additional IT resources. For a complete list of signature updates released by Fluke Networks, including Karmetasploit, AirDrop, AirPWN, Device Broadcasting XSS SSID, Ad-hoc Station Broadcasting Free Public Wi-Fi SSID and more, please visit the AirWISE Community. For more information about AirMagnet Enterprise 9.0, please

visit Fluke Networks.

For more information, visit www.FlukeNetworks.com [1]

Posted by Janine E. Mooney, Editor

January 24, 2012

Source URL (retrieved on *10/23/2014 - 12:33am*):
http://www.wirelessdesignmag.com/news/2012/01/fluke-networks-releases-new-signatures-protect-against-wlan-vulnerabilities?qt-digital_editions=0

Links:
[1] http://www.FlukeNetworks.com