Fluke Networks Releases New Signature Updates to Protect Against Emerging Wireless Security Threats and Vulnerabilities
Tuesday, November 08, 2011 03:38:57 PM (GMT)

AirMagnet's Intrusion Research Team monitors latest threats
creates custom signatures and automatically pushes updates to ensure AirMagnet Enterprise 9.0 customer protection

EVERETT, Wash., Nov. 8, 2011 /PRNewswire/ -- Fluke Networks today announced the release of new threat signature updates for its AirMagnet Enterprise 9.0 wireless intrusion detection and prevention system (WIDS/WIPS). The updates offer protection against wireless threats and vulnerabilities, including Karmetasploit and Apple's new AirDrop feature. By utilizing its proprietary Dynamic Threat Update (DTU) technology, AirMagnet Enterprise offers the only wireless LAN (WLAN) security system on the market today that can quickly generate signature updates for immediate protection and automatically push them to customers without requiring scheduled downtime or additional IT resources.

"Our ability to immediately update against emerging threats is increasingly critical to both our enterprise and government customers given the growth in Wi-Fi networks and cybercrime," said Jesse Frankel, product marketing manager at Fluke Networks and leader of the AirMagnet Intrusion Research Team. "In the last few months alone, the National Institute of Standards and Technology released updated security guidelines recommending that Federal agencies implement continuous monitoring in support of WLAN security – which they are now viewing as even more important than security monitoring for other types of systems(1)."

To help protect AirMagnet Enterprise customers against the changing WLAN vulnerabilities and threats, the following new signature updates have been released:

- **AirDrop** – Apple's Mac OS® X Lion includes the new AirDrop feature that allows multiple users to share files wirelessly – which can be a violation of company security policies – creating security risks that could result in protected data being easily transferred to unknown machines outside of the enterprise network, potentially leaving the network vulnerable to other active attacks.
- **Karmetasploit** – This is an aggressive man in the middle (MitM) style attack that tricks a client into associating with a device masquerading as an access point running KARMA. This allows a hacker to do any number of the following: gain access to the client machine, capture passwords, harvest data and conduct a wide variety of application exploits.
- **DHCP Starvation Attack** – A DHCP starvation attack run from a wireless client can cause other clients to connect to a malicious network. Wireless guest networks and unencrypted commercial hotspots are especially vulnerable to this attack, which can lead to lost productivity or revenue.

"The emergence of new threats and vulnerabilities like AirDrop, along with the evolution of sophisticated attack tools like Karmetasploit and viral SSIDs such as Free Public Wi-Fi, continue to prey upon wireless users who unwittingly expose corporate data and place their employer's assets at risk," said Lisa Phifer, president of network security consultancy Core Competence. "New WIPS signatures are essential to quickly being able to alert IT of such attacks. An up-to-date, always-available WIPS, such as AirMagnet Enterprise, can help enterprises avoid costly data breaches and WLAN downtime that may result from otherwise-undetected threats such as these."

For a complete list of signature updates released by Fluke Networks, including AirPWN, Device Broadcasting XSS SSID and Ad-hoc Station Broadcasting Free Public Wi-Fi SSID, please visit the AirWISE Community. For more information about AirMagnet Enterprise 9.0, please visit Fluke Networks.

About Fluke Networks

Fluke Networks is the world-leading provider of network test and monitoring solutions to speed the deployment and improve the performance of networks and applications. Leading enterprises and service providers trust Fluke Networks' products and expertise to help solve today's toughest issues and emerging challenges in WLAN security, mobility, unified communications and data centers. Based in Everett, Wash., the company distributes products in more than 50 countries. For more information, visit www.FlukeNetworks.com or call +1 (425) 446-4519.

(1) National Institute of Standards and Technology. September 2011. "Guidelines for Securing Wireless Local Area Networks (WLANs), Special Publication 800-153 (Draft)."

SOURCE Fluke Networks

Contacts: Kerry Desberg of Fluke Networks, +1-425-231-9529, Kerry.desberg@flukenetworks.com; or Justin Hall of VOXUS PR, +1-253-444-5442, jhall@voxuspr.com, for Fluke Networks
Countries: United States
Industries: Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: AAPL-US, 05M819-E
Related Identifiers: AAPL-US, 05M819-E
Subjects: New Products & Services