SkyJack Exploit and Vulnerability

The AirMagnet Intrusion Research Team recently discovered a new wireless vulnerability in Cisco wireless infrastructure. The vulnerability is connected to Cisco's "over the air provisioning" feature found in its wireless access points. This feature allows a newly deployed Cisco AP to listen to traffic from other nearby Cisco APs and use that information to quickly find a nearby WLAN controller. There are two sides of the vulnerability: First, there is an exposure or leakage of information that most users are not aware of and did not intend that is present in all lightweight Cisco APs. Secondly, while the over the air provisioning feature is enabled, there is the potential for APs to be incorrectly assigned to an outside Cisco controller (aka SkyJacked) either by accident or at the direction of a potential hacker.

A summary of key facts is listed below:

The Exposure

- In their normal operation, Cisco APs generate an unencrypted multicast data frame that travels over the air that includes a variety of information in the clear.
- From these frames a hacker listening to the airwaves could determine the MAC address of the wireless controller that the AP is connected, the IP address for that controller and a variety of AP configuration options.
- These frames are always unencrypted regardless of the encryption scheme used in the network.
- These frames are always sent regardless of whether the over the air provisioning feature is turned on or not
- At the very least, this allows anyone listening to the network to easily find the internal addresses of wireless LAN controllers in the network and potentially target them for attack.
- All lightweight Cisco deployments are subject to this exposure

Potential Exploits

- Unlike the vulnerability, the SkyJack exploit would require the over the air provisioning feature to actually be enabled.
- With the feature enabled, a newly deployed Cisco AP will listen to the above-mentioned Multicast Data Frame to determine the address of its nearest controller.
- The potential exists for the Cisco AP to "hear" multicast traffic from a neighboring network and incorrectly connect to a neighbor or otherwise unapproved Cisco controller.
- This ultimately could lead to an enterprise's access point connecting outside of the company to an outside controller and therefore under outside control.
- This same mechanism could be done intentionally by a hacker to purposely SkyJack APs, essentially taking over an enterprise access point.

Why It's Important

- All lightweight Cisco APs will expose the controller information and there is no way to turn the feature off.
- The exploit is potentially very damaging as it would have the effect of essentially turning an approved access point into a rogue and create an open a serious hole to the outside world.

Next Steps

At the present time, AirMagnet recommends that Cisco customers do not run the over the air provisioning as it could actively put new sensors in danger of being skyjacked. Customers should also leverage a dedicated independent IDS system capable of detecting wireless snooping and hacking tools to alert staff to the potential of an impending exploit. Furthermore, staff should such a monitoring system to validate that all corporate APs detected over the air are actually represented at the WLAN controller as any corporate AP that is not associated to a controller could be a serious security risk.

View Cisco Alert for more information from Cisco
http://tools.cisco.com/security/center/viewAlert.x?alertId=18919

About AirMagnet

AirMagnet Inc., now part of Fluke Networks, is the leader in security, performance and compliance solutions for wireless LANs. The company's innovative products include AirMagnet Enterprise, the leading 24x7 WLAN security and performance management solution, and AirMagnet WiFi Analyzer – which is known as the "de facto tool for wireless LAN troubleshooting and analysis." Other products provide WLAN site survey and design, RF interference detection, remote diagnostics, and the world's first voice over Wi-Fi analysis solution. AirMagnet has more than 8,500 customers worldwide, including 75 of the Fortune 100.

Corporate Headquarters
830 E. Arques Avenue
Sunnyvale, CA 94085
United States
Tel: +1 408.400.1200
Fax: +1 408.744.1250
www.airmagnet.com

EMEA Headquarters
6-9 The Square
Stockley Park
Uxbridge

Middlesex, UB11 1FW
Tel: +44 203 178 7926
Fax: +44 870 139 5156