US-CERT says Wi-Fi hole open to brute force attack

29 December 2011, by Nancy Owano

(PhysOrg.com) -- The US Computer Emergency Readiness Team (US-CERT) has issued a warning about a security hole in the Wi-Fi Protected Set-up protocol for Wi-Fi routers. Security researcher Stefan Viehbock discovered the vulnerability, reported it to the US-CERT, which then issued its public warning earlier this week. Viehbock was able to recognize design decisions about the protocol, which enables an efficient brute force attack.

The US-CERT warning said:

"The WiFi Protected Setup (WPS) PIN is susceptible to a brute force attack. A design flaw that exists in the WPS specification for the PIN authentication significantly reduces the time required to brute force the entire PIN because it allows an attacker to know when the first half of the 8 digit PIN is correct. The lack of a proper lock out policy after a certain number of failed attempts to guess the PIN on some wireless routers makes this brute force attack that much more feasible."

The protocol, introduced in 2007 by the Wi-Fi Alliance, was intended to make life simple for setting up and configuring security on wireless local area networks, especially for home and small office-home (SOHO) environments. "Wi-Fi Protected Setup enables typical users who possess little understanding of traditional Wi-Fi configuration and security settings to easily configure new wireless networks, to add new devices and to enable security," according to the WiFi Alliance white paper.

The simplification resides in the setup process where users only have to type in a shortened PIN instead of longer phrase if adding a new device to a network. By entering the wrong PIN, the hacker gets returned information that could be useful for an attack. The 8-digit PIN's security falls dramatically as more attempts are made. A message sent by the router when the PIN fails informs the hacker if the first four digits are correct; the last digit of the key is used as a checksum and is given out by the router in negotiation.

According to reports, this hole cuts the hacker's time and effort significantly. There is less effort in trying out combinations, reducing attempts from 100 million to 11,000.

In its warning, the US-CERT site said "We are currently unaware of a practical solution to this problem."

Its recommended workaround was to disable WPS. Though not a solution, it said a recommendation was to only use WPA2 encryption with a strong password, disabling UPnP, and enabling MAC address filtering so only trusted computers and devices can connect to the wireless network.

Affected vendors include Belkin, Buffalo, D Link, Linksys, Netgear, Technicolor, TP-Link, and

ZyXEL.

Viehbock, meanwhile, said he was working on a brute force tool, which he may release once he works the code into better shape.

More information:
www.kb.cert.org/vuls/id/723755
sviehb.wordpress.com/

APA citation: US-CERT says Wi-Fi hole open to brute force attack (2011, December 29) retrieved 24 June 2021 from https://phys.org/news/2011-12-us-cert-wi-fi-hole-brute.html