WiFi Protected Setup (WPS) PIN brute force Vulnerability

Ref ID	NCIT-SB-2012-03	**Vulnerability Identifier**	Stefan Viehböck
Description	Wi-Fi Protected Setup (WPS) is a Wi-Fi Alliance specification (v1.0 - available since January 2007) designed to ease the process of securely setup Wi-Fi devices and networks. An attacker within range of the wireless access point may be able to brute force the WPS PIN and retrieve the password for the wireless network, change the configuration of the access point, or cause a denial of service.		
Impact	Confidentiality **(High)**	Integrity **(High)**	Availability **(High)**
Vulnerability Type	Wireless Network Access (WPS PIN Disclosure, WPA Passphrase retrieval)		
Release Date	February 09, 2012	**Last Update Date**	March 25, 2012

Summary:

Viehbock reported the Wi-Fi Protected Setup (WPS) PIN brute force vulnerability to the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT). The Vulnerability allows an attacker to brute force the WPS PIN. Once you have the WPS pin you can instantly recover the WPA passphrase, even if the owner changes the passphrase.

Affected Vendors

Wi-Fi Protected Setup (WPS) is enabled by default on most major brands of wireless routers including Belkin, Buffalo, D-Link, Cisco's Linksys and Netgear, leaving millions of wireless routers around the world vulnerable to brute force attacks which can crack the Wi-Fi router's security in two to ten hours.

Solution:

1. Disable Wireless Protected Setup from the Router’s configuration Menu.

References

http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps

http://isc.sans.edu/diary.html?storyid=12292