Written by Bob Snyder
03 January 2012

The current Wifi Protected Setup (WPS) standard has a major vulnerability affecting millions of devices worldwide, according to security researcher Stefan Viehbock and the US Computer Emergency Readiness Team (US-CERT).

The researchers say a security hole allows one to access a WPS PIN-protected network in around 2 hours through the use of "brute force," since routers send a message informing potential hackers if the first 4 digits are correct while using the last digit of the key as a checksum. This reduces the 100 million security possibilities WPS should represent to around 11000.

WPS is popular among router manufacturers as a means for adding new devices to a wifi network without the need to remember a wireless key every time.

US-CERT suggests users should disable WPS on their routers, while Viehbock says routers from vendors including Buffalo, D-Link, Linksys and Netgear are vulnerable to such attacks-- but the manufacturers are ignoring his warnings. The researcher now plans to release a brute force tool, forcing vendors to resolve the issue.

Go Stefan Viehbock's Blog

Go US-CERT Security Warning