WiFi Protected Setup (WPS) PIN brute force vulnerability

Vulnerability Note VU#723755

Original Release Date: 2011-12-27 | Last Revised: 2012-05-10

Overview

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 many wireless routers makes this brute force attack that much more feasible.

Description

WiFi Protected Setup (WPS) is a computing standard created by the WiFi Alliance to ease the setup and securing of a wireless home network. WPS contains an authentication method called "external registrar" that only requires the router's PIN. By design this method is susceptible to brute force attacks against the PIN.

When the PIN authentication fails the access point will send an EAP-NACK message back to the client. The EAP-NACK messages are sent in a way that an attacker is able to determine if the first half of the PIN is correct. Also, the last digit of the PIN is known because it is a checksum for the PIN. This design greatly reduces the number of attempts needed to brute force the PIN. The number of attempts goes from 10^8 to 10^4 + 10^3 which is 11,000 attempts in total.

It has been reported that many wireless routers do not implement any kind of lock out policy for brute force attempts. This greatly reduces the time required to perform a successful brute force attack. It has also been reported that some wireless routers resulted in a denial-of-service condition because of the brute force attempt and required a reboot.

Impact

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.

Solution

We are currently unaware of a practical solution to this problem. Please consider the following workarounds:

Disable WPS

Within the wireless router's configuration menu, disable the external registrar feature of WiFi Protected Setup (WPS). Depending on the vendor, this may be labeled as external registrar, router PIN, or WiFi Protected Setup.