Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-UNAM-CERT-2012-01 Wi-Fi Protected Setup (WPS) Vulnerable a ataques de fuerza bruta

Wi-Fi Protected Setup (WPS) proporciona mecanismos simplificados para configurar la seguridad de redes inalámbricas. El mecanismo externo de intercambio de PIN es susceptible a ataques de fuerza bruta que podrían permitir a un atacante obtener acceso a la red Wi-Fi cifrada.

- **Fecha de Liberación:** 6-Ene-2012
- **Ultima Revisión:** 6-Ene-2012
- **Fuente:** US-CERT
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Mal diseño.

1. Descripción

WPS usa un PIN como secreto compartido para autenticar al Access Point con los clientes y proporciona información de la conexión como contraseñas y llaves. Durante el método de registro de intercambio externo, un cliente necesita proporcionar un PIN correcto al Access Point.

Un cliente atacante puede tratar de adivinar el PIN correcto. Existe una vulnerabilidad de diseño que reduce el espacio de PIN de tal manera que permite ataques de fuerza bruta. Herramientas gratuitas de ataque pueden obtener un PIN de 4 a 10 horas.
Para más información, revisar la Vulnerabilidad VU#723755

2. Impacto

Un atacante dentro de un radio aceptable puede realizar un ataque de fuerza bruta al PIN WPS de un Access Point vulnerable. El atacante puede obtener las contraseñas WEP o WPA y obtener acceso a la red Wi-Fi. Una vez en la red, el atacante puede monitorear el tráfico y realizar nuevos ataques

3. Solución

Actualizar el Firmware

Visite el sitio del vendedor del Access Point para obtener el firmware actualizado que corrige esta vulnerabilidad. Para más información revisar la proporcionada por el vendedor para la vulnerabilidad VU#723755 y en Google spreadsheet como WPS Vulnerability Testing.

Deshabilitar WPS

Dependiendo del Access Point, podría ser posible dehabilitar WPS. Tomar en cuenta que algunos Access Point podrían no deshabilitar WPS aún cuando en la interfaz de administración indique que WPS está deshabilitado.

4. Referencias

* Vulnerability Note VU#723755 -
<http://www.kb.cert.org/vuls/id/723755>

* Wi-Fi Protected Setup PIN brute force vulnerability
- <http://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/>

* Cracking WiFi Protected Setup with Reaver -
<http://www.tacnetsol.com/news/2011/12/28/cracking-wifi-protected-setup-with-reaver.html>

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Pablo Antonio Lorenzana Gutiérrez (plorenzana at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47