Magnet Networks - Weak WPA-PSK Passphrases in Tesley CPVA 642

Exploit Title: Magnet Networks – Weak WPA-PSK passphrases used in Tesley CPVA 642 Router
Google Dork:
Date: 01/06/2016
Author: Matt O'Connor
Advisory Link: https://www.rgb.ie/magnet-broadband-weak-wpa-psk-algorithm.pdf
Version:
Category: Remote
Tested on: Magnet Networks Tesley CPVA 642

The Tesley CPVA 642 routers supplied by Magnet Networks are vulnerable to an offline dictionary attack if the WPA-PSK handshake is obtained by an attacker.

The WPA-PSK pass phrase has the following features:

- Starts with MAGNET0
- Adds six random numerical digits
- 1 million possible combinations (MAGNET0000000 – MAGNET0999999)

The entire keyspace can be generated using “mask processor” by ATOM, piping each letter out to its own file, for example:

```
./mp32 MAGNET0?1?1?1?1?1?1 > magnet_networks_tesley_ks.txt
```

The .txt file weighs in at around 45mb.

Using a 1.4ghz i3 processor on a budget laptop, we were hitting 1,000 keys per second. Breakdown below:

- 1,000,000 / 1,000 keys per second = 1,000 seconds
- 1,000 / 60 seconds = 16~ minutes

The WPA-PSK handshake we used has the password MAGNET0349325 and was cracked within ~6 minutes.

If you’re using the default password on your Magnet Networks Tesley CPVA 642 Router, we recommend changing it immediately to a more secure password, using a mix of letters, numbers and symbols.

On the 20th of June 2016, Magnet Networks Customer Care confirmed via email that these routers are not used by Magnet Networks anymore.