# Exploit Title: UPC Ireland Cisco EPC 2425 Router / Horizon Box
# Google Dork:
# Date: 11/12/2013
# Author: Matt O'Connor / Planit Computing
# Advisory Link: http://www.planitcomputing.ie/upc-wifi-attack.pdf
# Version:
# Category: Remote
# Tested on: Cisco EPC 2425 / Horizon Box

The Cisco EPC 2425 routers supplied by UPC 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:

- Random
- A to Z Uppercase only
- 8 characters long
- 208,827,064,576 possible combinations (AAAAAAAA – ZZZZZZZZ) 26^8

We notified UPC about the problem in November 2011 yet UPC are still supplying customers with newer modems / horizon boxes that use this algorithm.

At the time, graphics cards were expensive and clustering several machines was not financially viable to the average hacker.

We recently purchased a used rig, comprising off:

- Windows 7
- I3 Processor
- 4GB RAM
- 2TB Drive
- Radeon HD 5850

We generated 26 dictionary files using “mask processor” by ATOM, piping each letter out to its own file, for example:

```
A:  ./mp32 A?u?u?u?u?u?u?u > A.TXT = AAAAAAAA – AZZZZZZZ

B: ./mp32 B?u?u?u?u?u?u?u > B.TXT = BAAAAAAA – BZZZZZZZ
```

etc

Each .txt file weighed in at around 60GB’s each. The 26 files took up about 1.6TB of storage.

We now had the complete key space, partitioned into 26 different files. This allowed us to distribute the brute force attack amongst multiple computers. There are other ways with ocl-hashcat but this was the simplest.

Using our Radeon HD5850 on standard settings, we were hitting 80,000 keys per second. Breakdown below:

- 26^8 = 208,827,064,576 (208 billion possible combinations)
- 26^8 / 80,000 keys per second = 2,610,338 seconds
- 2,610,338 / 60 seconds = 43,505 minutes
- 43,505 / 60 minutes = 725 hours
- 725 hours / 24 hours = 30 Days

For €185, we had built a computer that could crack the default UPC wireless password within 30 days. The WPA-PSK handshake we used started with the letter D and was cracked within 96 hours.

We ended up getting a second machine for the same price which resulted in our maximum cracking time being reduced to 15 days.

If you’re using the default password on your UPC broadband connection, we recommend changing it immediately to a more secure password, using a mix of letters, numbers and symbols.