Hack Forums

Hack Forums > Hacks, Exploits, and Various Discussions > Wifi WPA WEP Bluetooth 4G LTE Wireless Hacking > List of Default WPS PIN
Full Version: List of Default WPS PIN
You're currently viewing a stripped down version of our content. View the full version with proper formatting.
Pages: 1 2 3 4 5 6 7 **8** 9 10

Kara Davis

02-03-2015, 01:26 PM
Its not possible to generate the default pins for Thomson / Technicolor. Simply because no one figured how those are generated.

If the default psk has been changed as you suspect, you can try to crack those handshakes, or a Fake AP.
Wps is very hard to break with newer firmwares on TG784, its still possible but takes ages. (10 attempts is not too bad if the lock goes away, there are harder firmwares)

vit07

02-04-2015, 10:40 AM
Thanks very much for your reply...
I think I will try the Fake AP, because in the Handsake I think I must have a dictionary. If the dictionary doesn´t have the word is waste of time.
I write this post because I saw somethig write about the thomson tg784 with the MAC and the WPS PIN.
Maybe Some Member wrote the thomson MAC, WPS PIN, that he had in his possession and wasn´t calculated.

I send some data about thomson tg784.

I hope that can help someone that wishes to find an algorithm for thomson.

Thomson tg 784

MAC 00:1F:9F:7D:D1:11
WPS PIN 16069749

MAC 00:1F:9F:D9:E9:E8
WPS PIN 65689202

Thomson tg 784n
MAC 58:98:35:7D:7B:64
WPS PIN 30929272
SN: CP1202NT0VG

vit07

02-10-2015, 01:15 PM
Hi community!
Can anyone get me the WPS PIN for this MAC 38:22:9D:BE:A8:46 ?
It's a Pirelli.
Thanks

izzydak1d

03-25-2015, 06:57 AM
Can anybody help with the pin to netgear09

h4x0rm1k3

03-25-2015, 08:07 AM

> *(03-25-2015 06:57 AM)izzydak1d Wrote: [->]*Can anybody help with the pin to netgear09

There's a dictionary with about 16 million passwords for the NETGEARXX routers, if you can get the handshake, use ohashcat with that dictionary it wouldn't take too long to run through them all even if you were just using CPU power! If that doesn't work then I think you're out of luck i'm afraid!

> *(02-10-2015 01:15 PM)vit07 Wrote:* [->]Hi community!
> Can anyone get me the WPS PIN for this MAC 38:22:9D:BE:A8:46 ?
> It's a Pirelli.
> Thanks

Hex to Dec calculator is what you need to try and decipher them, just use the last 6 octets of the MAC & pop it into windows programmer calculator and then hit Dec and it'll convert it for you. Anyway, it spat out 12494918 which may work, if not try knocking the 1st 1 off & try that, also try it with 0 in it's place & also try 0 at the end as they sometimes work (particularly when Hex2Dec only converts to 7 digits or it's 8 digits and but starts with a 0 and in that case you take out the 0) I hope that makes sense, it does in my spacious mind anyway! I also hope the conversion worked for you, if it does then please report back for other Pirelli users to find.

Kara Davis

03-25-2015, 02:44 PM

> *(02-04-2015 10:40 AM)vit07 Wrote:* [->]Thomson tg 784
>
> MAC 00:1F:9F:7D:D1:11
> WPS PIN 16069749
>
> MAC 00:1F:9F:D9:E9:E8
> WPS PIN 65689202

Its possible to calculate the default psk from ssid if manufactered before 2009 try here http://www.nickkusters.com/en/services/t...speedtouch

if ssid is same of mac adress means is from 2010 and you cant calculate the psk from ssid but you can generate a 28mb dictionary and crack it. look for "wifipassreminder" script

> *(02-10-2015 01:15 PM)vit07 Wrote:* [->]Can anyone get me the WPS PIN for this MAC 38:22:9D:BE:A8:46 ?

The default pin for those is 12345670, you need to use -w flag in reaver and have a very good signal for the router to respond. If pin was changed you can bruteforce it since there is no AP rate limit stuff at all.

vit07

04-20-2015, 08:10 AM
Just today see your replies...

To h4x0rm1k3
I already try reaver in the Pirelli and it arrives to the Pin start with 4******. And didn´t work with any PIN. But I will try your sugestion. I went to Google and find a Hex to Dec calculator and the result was 12494918, like you said.

Thank you very much h4x0rm1k3

To Kara Davis
I already have the default psk calculator for thomson and it works if the pass isn´t changed. The reason that I want a PIN generator for thomson, is to find the Pass quickly with reaver or bully. With the dictionary I think is Impossible....
I found a wps pin of a TPlink and the PSK was "run my car to 100MHP". With the Wps pin I found the pass in 10 or 20 seconds... With a handshake I think is impossible

In the Pirelli, before I wrote this post, I already used that PIN 12345670 and didn´t work.
I already used the reaver and it arrives to 4******. Then my computer broke down and I stop the attack.
Sometimes the Pirelli had some stops and then I made a mdk attack. Only when the Pirelli change the channel I could have sucess in new attacks to get another PIN. I try it in 2 mounths then I stop the tries. I Had 45 to 55 signal and I used the -w flag.

By the way the PIN 12345670 is very used in the HOTBOX.

Thank you very much Kara Davis

Kara Davis

04-20-2015, 12:59 PM
Pirelli - mac sugests model P.DG A1000G , which comes with 12345670 as default pin, this model uses ralink chipset so should also be vulnerable to new pixiedust attack, that way you can calculate the pin. Make sure the WPS is enabled/configured and use -w argument with reaver. this info must do it.

Thomson - there is no PIN calculation for these models.
You can calculate the default psk with the program if the ssid is left default and if

the AP is from 2009 or earlier.
For changed ssids and 2010 APs (the ones where the ssid is the same as the mac) you must generate the wordlist of all possible default passwords and crack it, Its a 28mb per year list, this is the only way i know.
If its a technicolor model (from 2011 until now) i dont know of any major vulnerabilities. firmwares get updated remotely in this model, so they patched wps exploitation quickly.

rbeldua

04-21-2015, 12:04 PM
arcadyan technology corp.
wpspin is 00571111

anybody has a wpspin for huwei technology?

agentshield

04-28-2015, 07:28 PM
On Comcast/xfinity Router/Gateway the wps are calculated by coverting the last 6 values of the mac address from hec to dec. after converting you will get either a 7 or 8 digit answer. if u get 8 digit. drop the first value, then reaver it.

Proof
Pin cracked in 73 seconds
[+] WPS PIN: '23407282'
[+] WPA PSK: 'H21208270B275A94'
[+] AP SSID: 'HOME-B778'
[+] Nothing done,

Pages: 1 2 3 4 5 6 7 **8** 9 10
Hack Forums > Hacks, Exploits, and Various Discussions > Wifi WPA WEP Bluetooth 4G LTE Wireless Hacking > List of Default WPS PIN

Reference URL's

- **Hack Forums:** http://www.hackforums.net/index.php
- **:**