SECURITY IS A PROCESS, NOT A STATE • **CARVE SYSTEMS LLC**

Computers Everywhere!

April 2016

Outline

- About Carve
- IoT Landscape
- “Full Stack IoT”
- IoT assessment methodology
- Bugs!
- What can we do?

About Carve Systems

- Founded in 2011 by industry veterans
  - Specializing in full-stack risk assessment and deep-dive penetration testing
  - Hardware - Firmware/OS - Infrastructure - Applications
- Headquartered in NYC
  - Clients all over North America
- Research driven consulting
  - We are hardware/software engineers
- Speakers at BlackHat, Defcon, CanSecWest, OWASP

0xGROG

- Mike Zusman - Founder
  - 10,000 foot view
  - Thinker
  - Innovate
  - Develop new business

Artwork by Mike Ferrin for Carve Systems

0xGROG

- Max Sobell – Partner
  - Make sure the gears keep turning
  - Find shiny things
  - Bang them with rocks

- Why Grog?
  - Invent tools
  - Hard work
  - Don’t overcomplicate

Recent/Notable Public Work

- Qolsys IQ Panel contains multiple vulnerabilities VU#573848 (2015)
  - https://www.kb.cert.org/vuls/id/573848
  - Hardcoded Cryptographic Keys
    - https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6032
    - CVSS v2 Base Score: 9.3 (HIGH)
  - Failure to verify cryptographic signatures
    - https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6033
    - CVSS v2 Base Score: 9.3 (HIGH)
- CradlePoint local sandbox escape vulnerability (2015)
  - Release notes for CradlePoint Rev 6.0.1 Firmware (via CP portal)
  - http://www.tcisystems.biz/PDF/ReleaseNotes_S3_6_0_1.pdf
- ICANN “Dotless” Risk Assessment (2013) (not IoT/M2M)
  - https://www.icann.org/news/announcement-2013-08-05-en

https://www.kb.cert.org/vuls/id/573848
CERT | Software Engineering Institute | Carnegie Mellon University
DATABASE HOME
SEARCH
REPORT A VULNERABILITY
HELP
Print
Tweet
Send
Share

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

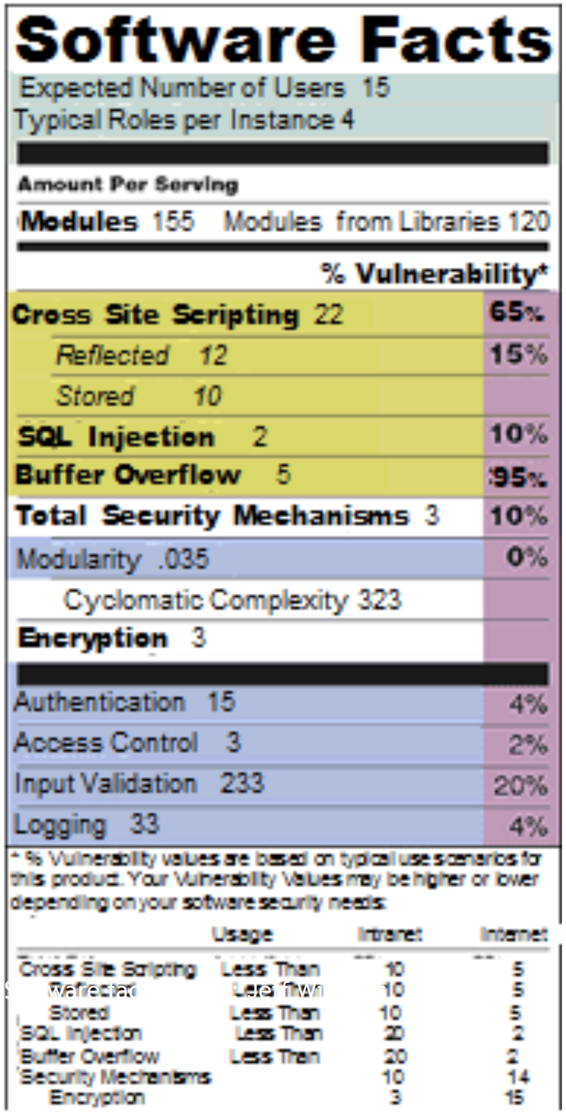
Vulnerability Note VU#573848

Qolsys IQ Panel contains multiple vulnerabilities

Original Release date: 29 Oct 2015 | Last revised: 29 Oct 2015

ICANN

2004 versus 2015/2016



Software Facts

Expected Number of Users 15
Typical Roles per Instance 4

Amount Per Serving

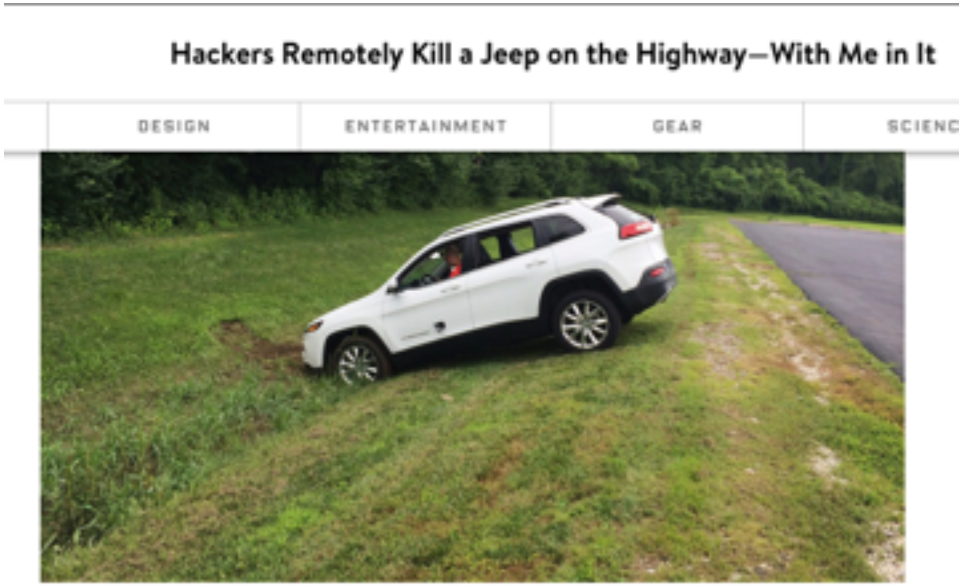
Modules 155 Modules from Libraries 120

	% Vulnerability*
Cross Site Scripting 22	**65%**
Reflected 12	15%
Stored 10	
SQL Injection 2	10%
Buffer Overflow 5	95%
Total Security Mechanisms 3	10%
Modularity .035	0%
Cyclomatic Complexity 323	
Encryption 3	
Authentication 15	4%
Access Control 3	2%
Input Validation 233	20%
Logging 33	4%

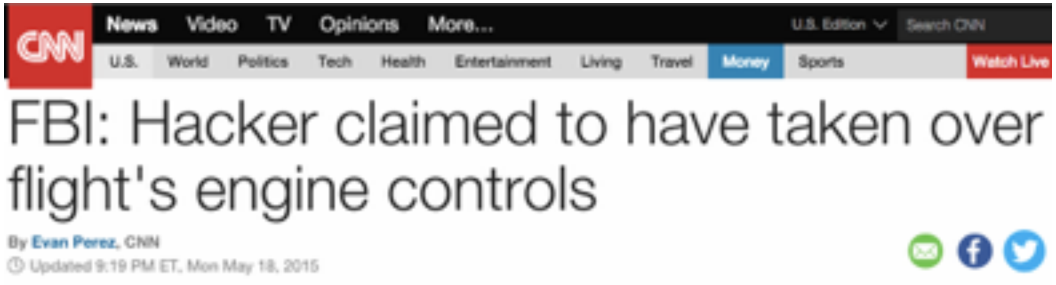
* % Vulnerability values are based on typical use scenarios for this product. Your Vulnerability Values may be higher or lower depending on your software security needs:

	Usage	Intranet	Internet
Cross Site Scripting	Less Than	10	5
Reflected	[illegible]	10	5
Stored	Less Than	10	5
SQL Injection	Less Than	20	2
Buffer Overflow	Less Than	20	2
Security Mechanisms		10	14
Encryption		3	15

Software Facts label credit to Jeff Williams



Hackers Remotely Kill a Jeep on the Highway—With Me in It



FBI: Hacker claimed to have taken over flight's engine controls

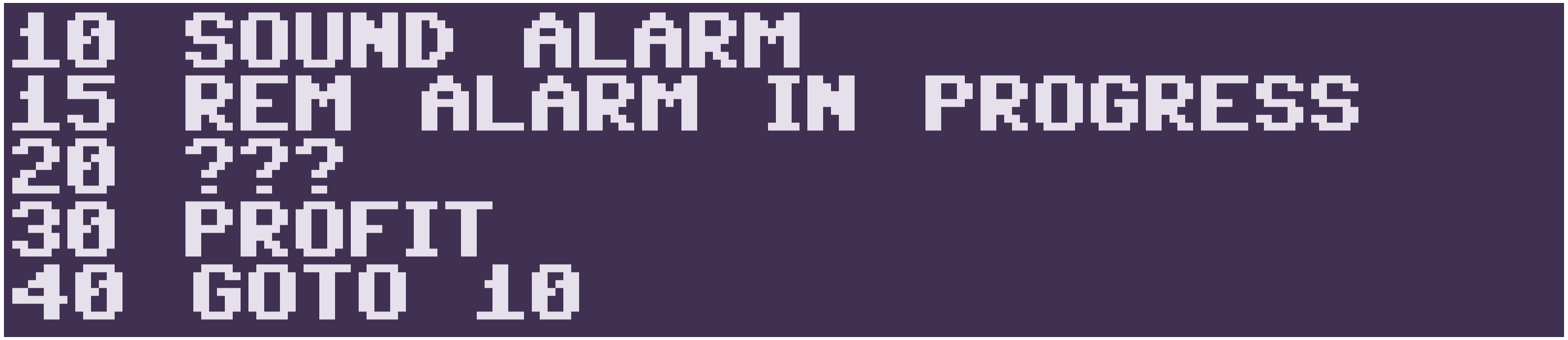
By Evan Perez, CNN
Updated 9:19 PM ET, Mon May 18, 2015

How many computers in this picture?

- Big Data
- IT vs OT (Operations Technology) (Manufacturing vs Operations)
- Predictive Analytics
- Predictive Maintenance -> Changes business models

What is IoT?

- “IoT is insecure!”
  - Everyone knows it.
  - Even your parents.
  - We’re tired of hearing it.



```
10  SOUND  ALARM
15  REM  ALARM  IN  PROGRESS
20  ???
30  PROFIT
40  GOTO  10
```

What is IoT?

- How IoT is marketed

SHINY

What is IoT?

- IoT Reality

What is IoT?

- IoT Device Profile

Primarily embedded systems (Linux)

16 – 512MiB RAM Common

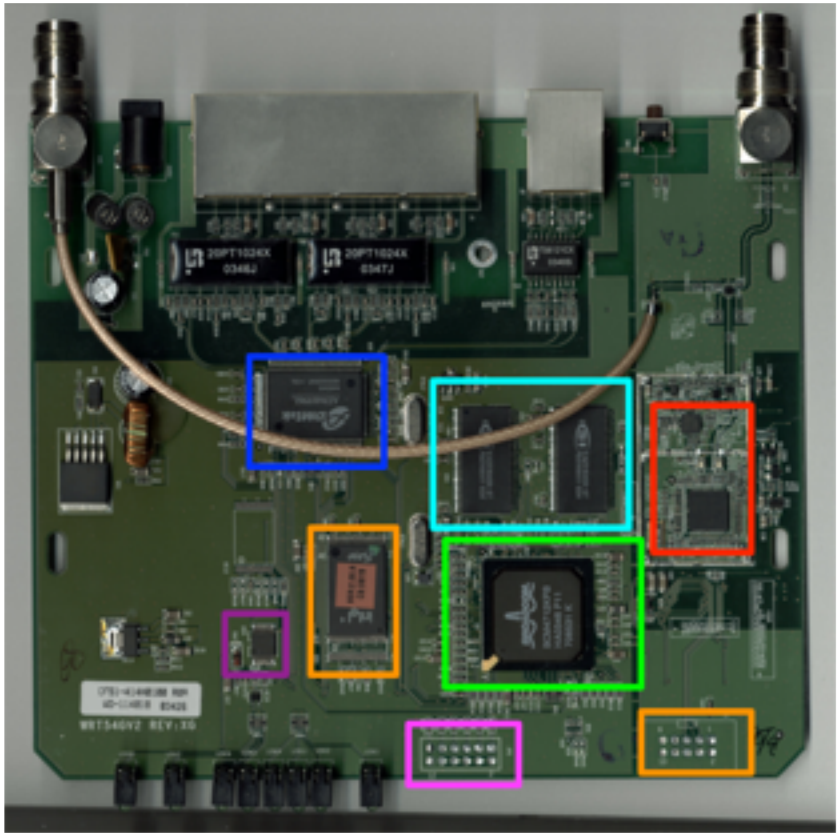
2-8 GiB Flash Storage Common

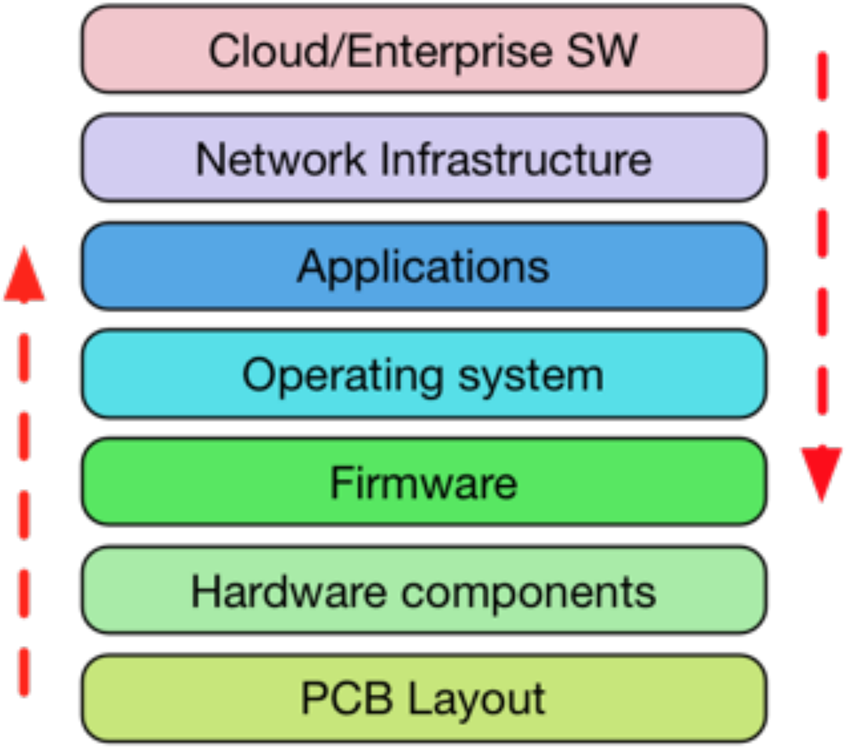
ARM Processors, Occasional X86 or MIPS

Internet Connected

Most have a management web application

Full Stack IoT





Cloud/Enterprise SW

Network Infrastructure

Applications

Operating system

Firmware

Hardware components

PCB Layout

IoT Software

- We’ve seen:
  - Web servers that let you “PUT” server-side scripts to set/reveal admin passwords
  - Countless command injections to root
  - Janky encryption routines that can be broken in practice (as opposed to only theoretical)
- First sacred tenant of Secure IoT development:

Don’t re-invent the wheel

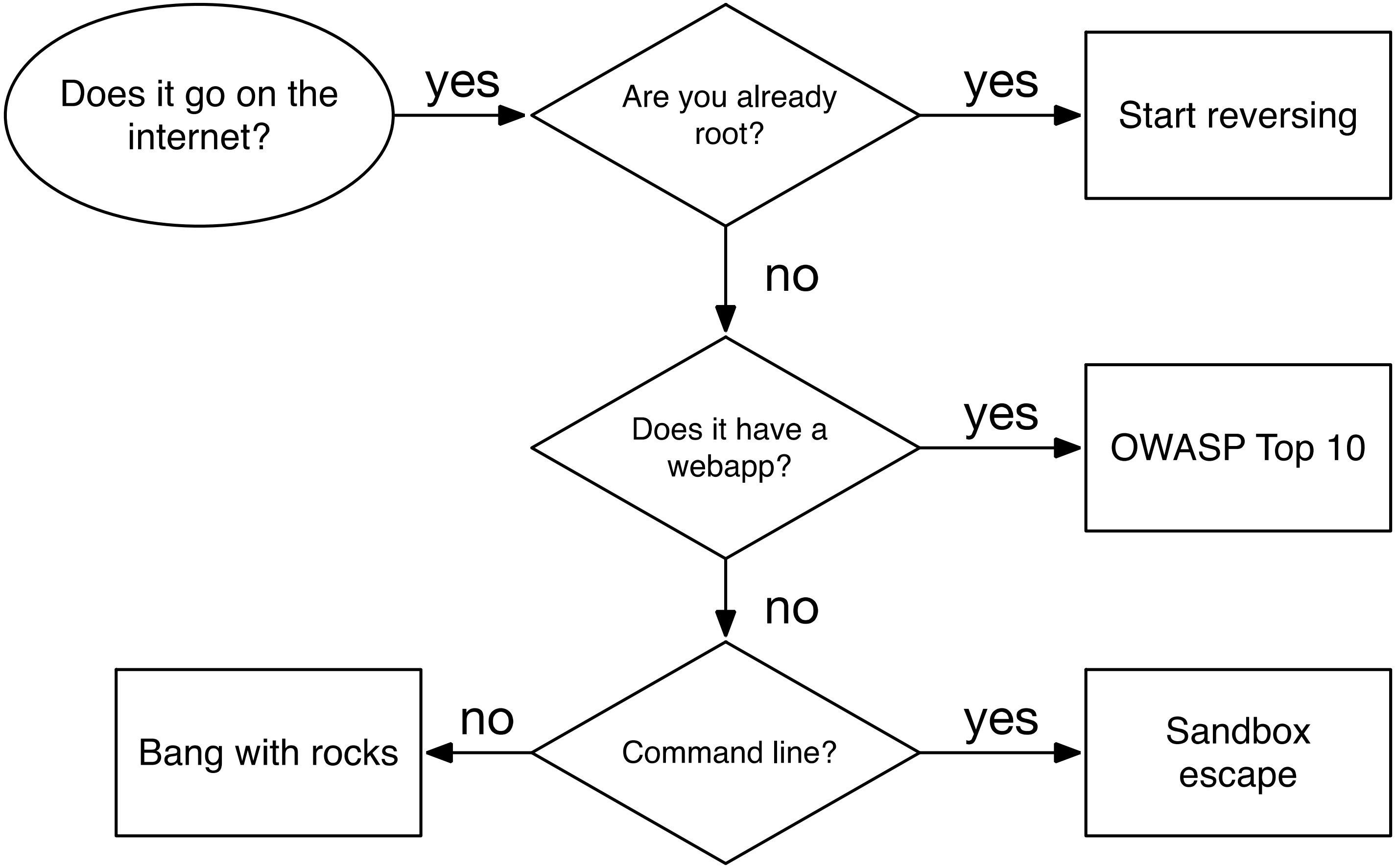
Odd command injection

- Ruggedized Router/Vehicle Tracker
- This thing has it all:
  - Web app flaws (auth bypass, command injection)
  - Insecure default settings
  - Awful cryptography
- Result: remote root exploit
  - Affects 100's or 1000's of devices on public networks

How do impactful bugs happen?

- The goal: using what you know about your device, get root on another device
- Start with the admin
  - How do they configure the device?
  - How do they monitor/interact?
- Can you download a firmware image?
  - Is the file system easy to mount and work? Encrypted?

IoT Methodology Cheat Sheet®



Step by step: root

- Assume the user is root
- Why would you already be root?
  - It's your device
  - If you're not already root, you will be shortly
- Second sacred tenant of IoT development:

Secrets from one device should not be shared with other devices

No Sharing

- Don’t trust these devices for a second
  - Privileged network access
  - Hard-coded keys (encryption, SSH)
  - Backdoor accounts
  - Updating
- Public case study #1: Updating

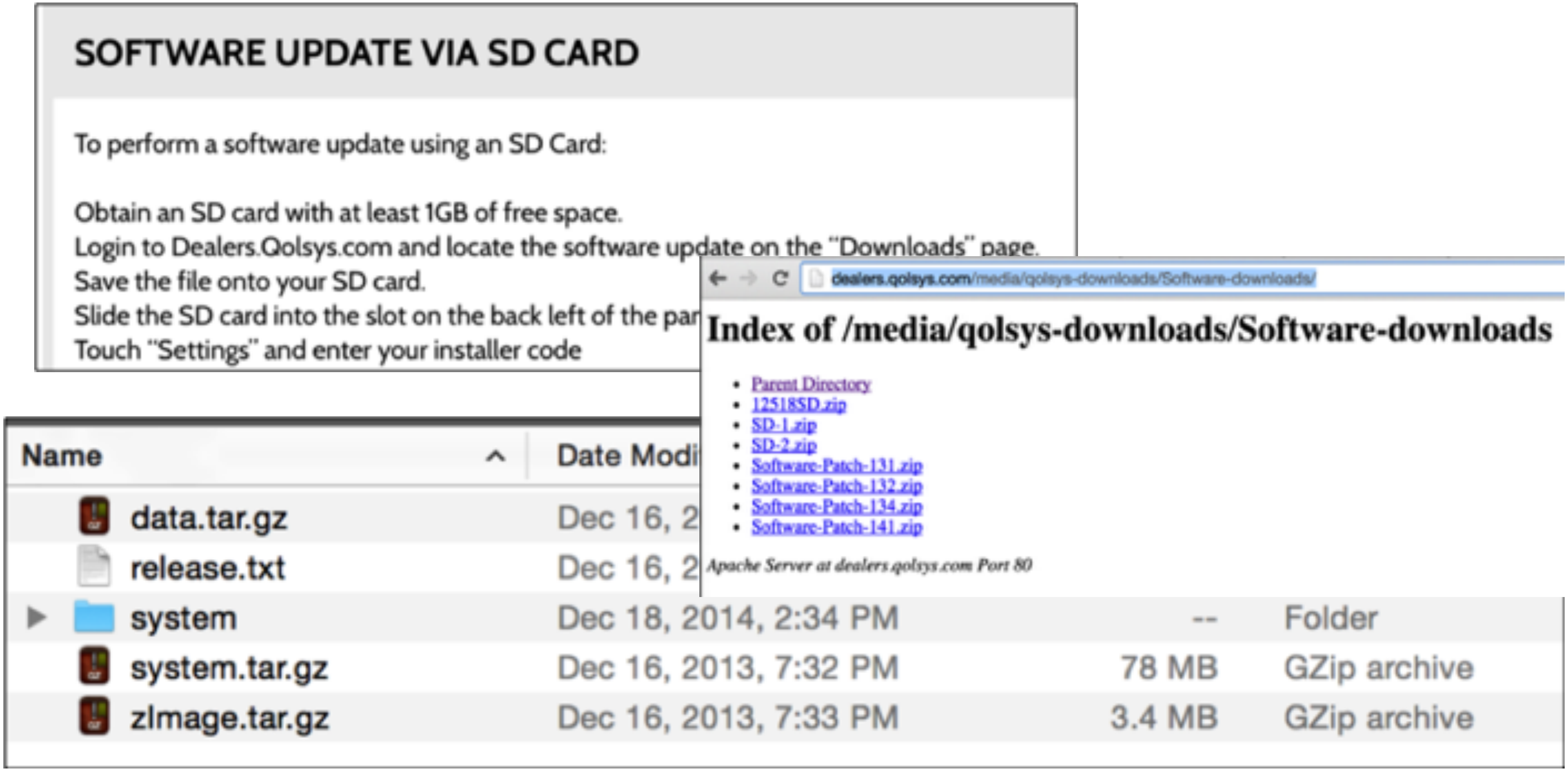
How doth one update?

- Home alarm system
  - Android
  - No web app, no admin config
  - No problem
- Dealer network
- Force-browse to the update package

CVE-2015-6032, 6033; https://www.kb.cert.org/vuls/id/573848
Thanks, CERT!

vuln credit: Roman @ Carve

via SD Card



SOFTWARE UPDATE VIA SD CARD

To perform a software update using an SD Card:

Obtain an SD card with at least 1GB of free space.
Login to Dealers.Qolsys.com and locate the software update on the "Downloads" page.
Save the file onto your SD card.
Slide the SD card into the slot on the back left of the par
Touch "Settings" and enter your installer code

dealers.qolsys.com/media/qolsys-downloads/Software-downloads/

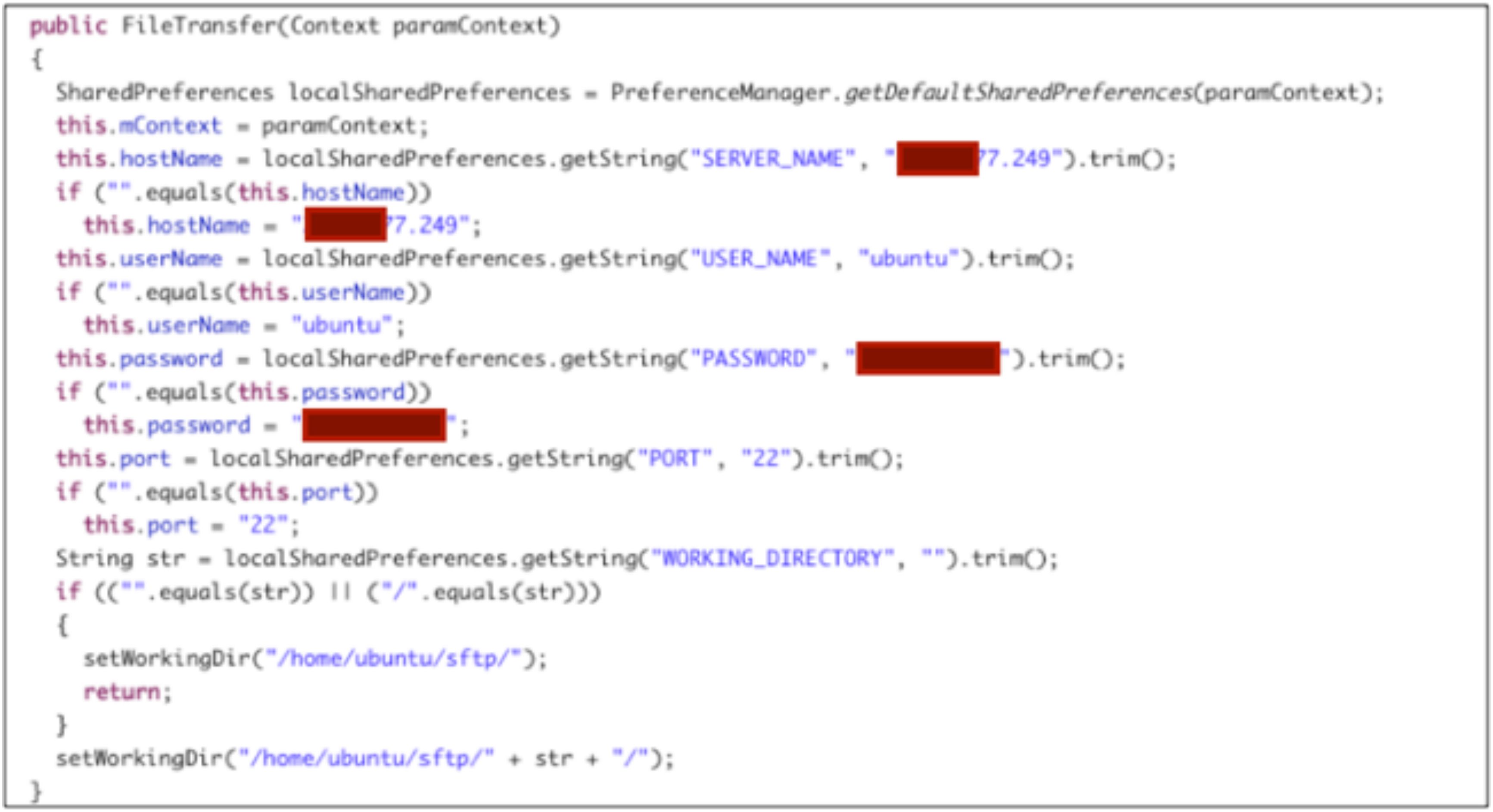
Index of /media/qolsys-downloads/Software-downloads

- Parent Directory
- 12518SD.zip
- SD-1.zip
- SD-2.zip
- Software-Patch-131.zip
- Software-Patch-132.zip
- Software-Patch-134.zip
- Software-Patch-141.zip

Apache Server at dealers.qolsys.com Port 80

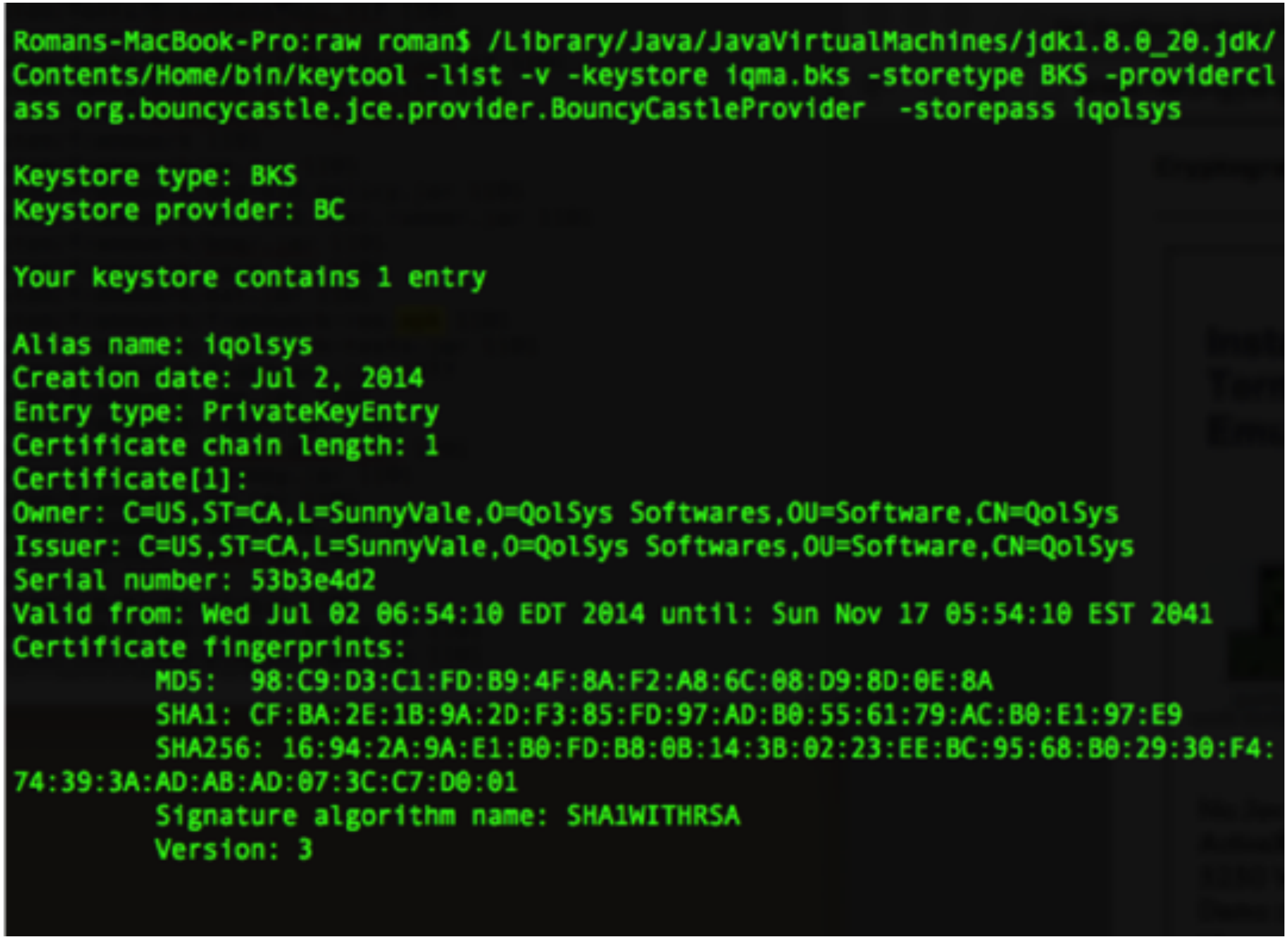
Name	Date Modi		
data.tar.gz	Dec 16, 2		
release.txt	Dec 16, 2		
system	Dec 18, 2014, 2:34 PM	--	Folder
system.tar.gz	Dec 16, 2013, 7:32 PM	78 MB	GZip archive
zImage.tar.gz	Dec 16, 2013, 7:33 PM	3.4 MB	GZip archive

Oh no…



```
public FileTransfer(Context paramContext)
{
  SharedPreferences localSharedPreferences = PreferenceManager.getDefaultSharedPreferences(paramContext);
  this.mContext = paramContext;
  this.hostName = localSharedPreferences.getString("SERVER_NAME", "[redacted]7.249").trim();
  if ("".equals(this.hostName))
    this.hostName = "[redacted]7.249";
  this.userName = localSharedPreferences.getString("USER_NAME", "ubuntu").trim();
  if ("".equals(this.userName))
    this.userName = "ubuntu";
  this.password = localSharedPreferences.getString("PASSWORD", "[redacted]").trim();
  if ("".equals(this.password))
    this.password = "[redacted]";
  this.port = localSharedPreferences.getString("PORT", "22").trim();
  if ("".equals(this.port))
    this.port = "22";
  String str = localSharedPreferences.getString("WORKING_DIRECTORY", "").trim();
  if (("".equals(str)) || ("/".equals(str)))
  {
    setWorkingDir("/home/ubuntu/sftp/");
    return;
  }
  setWorkingDir("/home/ubuntu/sftp/" + str + "/");
}
```

Private signing key

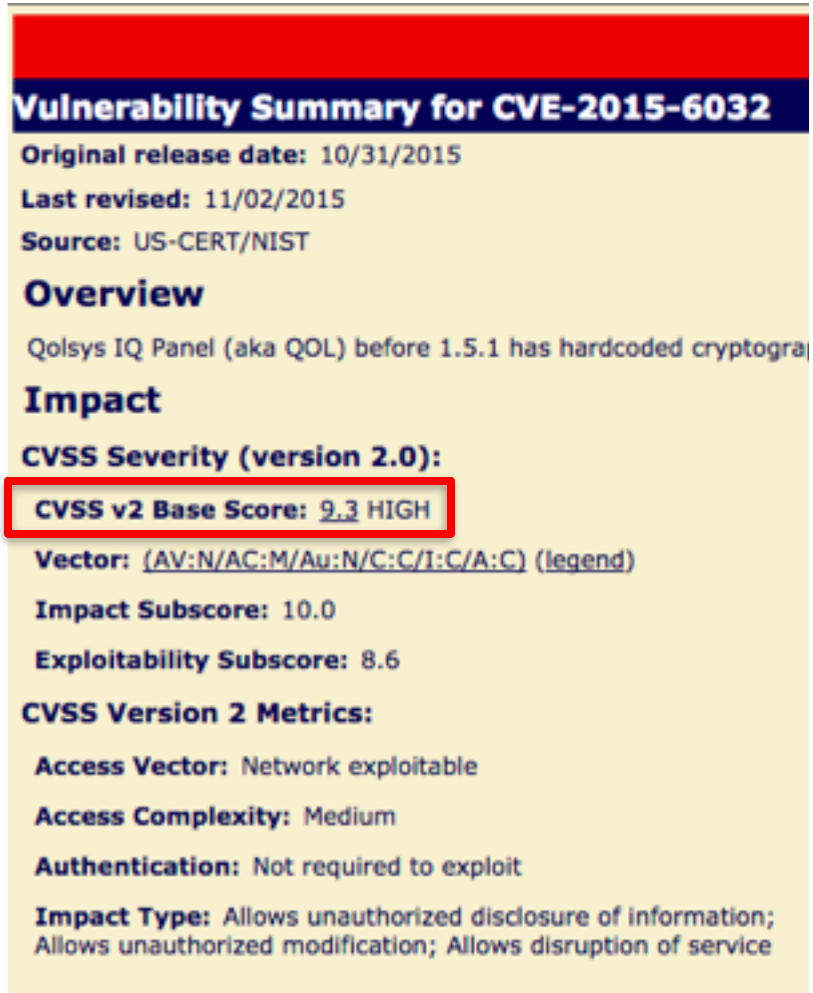


```
Romans-MacBook-Pro:raw roman$ /Library/Java/JavaVirtualMachines/jdk1.8.0_20.jdk/
Contents/Home/bin/keytool -list -v -keystore iqma.bks -storetype BKS -providercl
ass org.bouncycastle.jce.provider.BouncyCastleProvider  -storepass iqolsys

Keystore type: BKS
Keystore provider: BC

Your keystore contains 1 entry

Alias name: iqolsys
Creation date: Jul 2, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: C=US,ST=CA,L=SunnyVale,O=QolSys Softwares,OU=Software,CN=QolSys
Issuer: C=US,ST=CA,L=SunnyVale,O=QolSys Softwares,OU=Software,CN=QolSys
Serial number: 53b3e4d2
Valid from: Wed Jul 02 06:54:10 EDT 2014 until: Sun Nov 17 05:54:10 EST 2041
Certificate fingerprints:
         MD5:  98:C9:D3:C1:FD:B9:4F:8A:F2:A8:6C:08:D9:8D:0E:8A
         SHA1: CF:BA:2E:1B:9A:2D:F3:85:FD:97:AD:B0:55:61:79:AC:B0:E1:97:E9
         SHA256: 16:94:2A:9A:E1:B0:FD:B8:0B:14:3B:02:23:EE:BC:95:68:B0:29:30:F4:
74:39:3A:AD:AB:AD:07:3C:C7:D0:01
         Signature algorithm name: SHA1WITHRSA
         Version: 3
```

Attack scenario

- Attack scenario:
  - Create malicious update package
  - Sign with vendor private key
  - Log in + push update to vendor server [we did not try this]
  - All devices download malicious update package and install (key matches) [or this]
- This bug is now fixed – thanks to CERT for coordinating disclosure

CERT FTW



Vulnerability Summary for CVE-2015-6032

Original release date: 10/31/2015

Last revised: 11/02/2015

Source: US-CERT/NIST

Overview

Qolsys IQ Panel (aka QOL) before 1.5.1 has hardcoded cryptogra

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

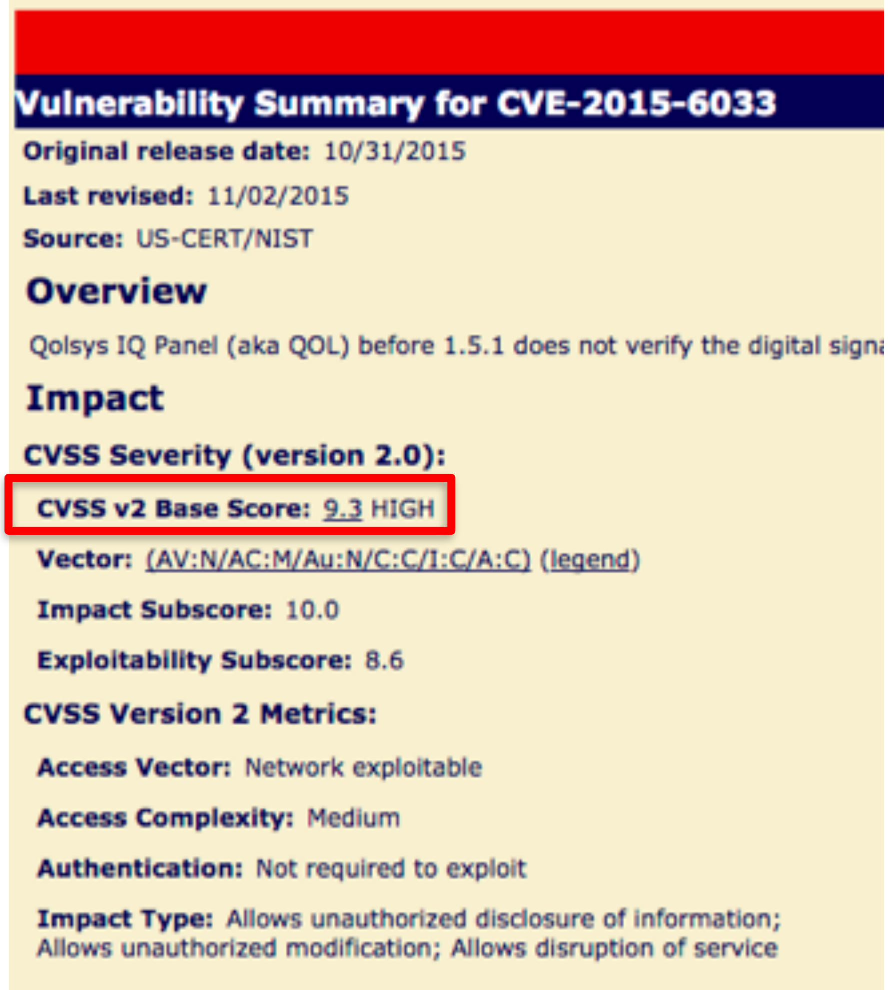
CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service



Vulnerability Summary for CVE-2015-6033

Original release date: 10/31/2015

Last revised: 11/02/2015

Source: US-CERT/NIST

Overview

Qolsys IQ Panel (aka QOL) before 1.5.1 does not verify the digital signa

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

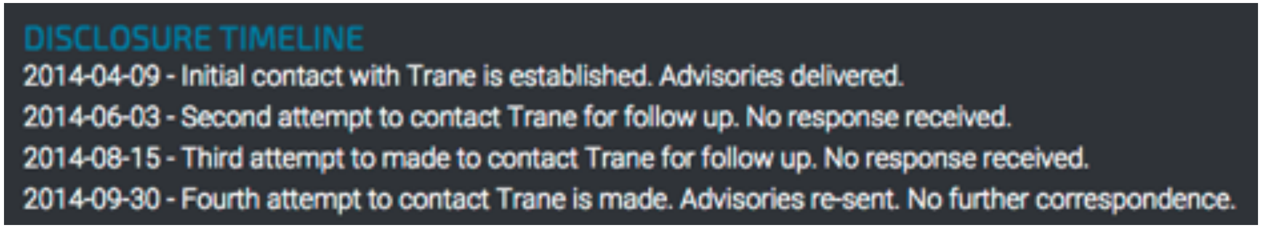
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

More on CERT

- They run a great service
- We prefer to disclose bugs to CERT first
- CERT will help coordinate disclosure if the vendor becomes unresponsive
  - (or if the world is going to end)
- They will **only** publish if they coordinate disclosure

We want more bugs!

- IoT fixes are slow. Not our timeline*:



DISCLOSURE TIMELINE

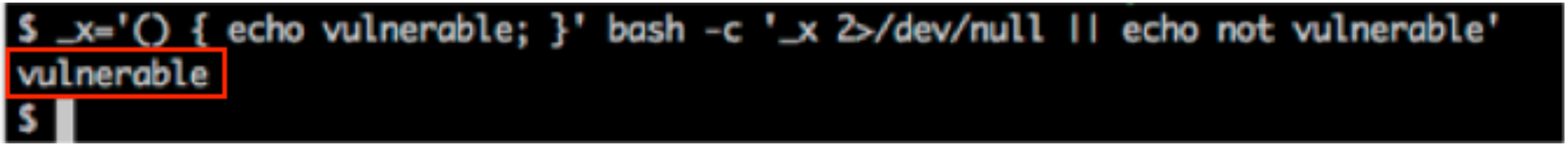
2014-04-09 - Initial contact with Trane is established. Advisories delivered.

2014-06-03 - Second attempt to contact Trane for follow up. No response received.

2014-08-15 - Third attempt to made to contact Trane for follow up. No response received.

2014-09-30 - Fourth attempt to contact Trane is made. Advisories re-sent. No further correspondence.

- Slow to patch. Slow to update.



```
$ _x='() { echo vulnerable; }' bash -c '_x 2>/dev/null || echo not vulnerable'
vulnerable
$
```

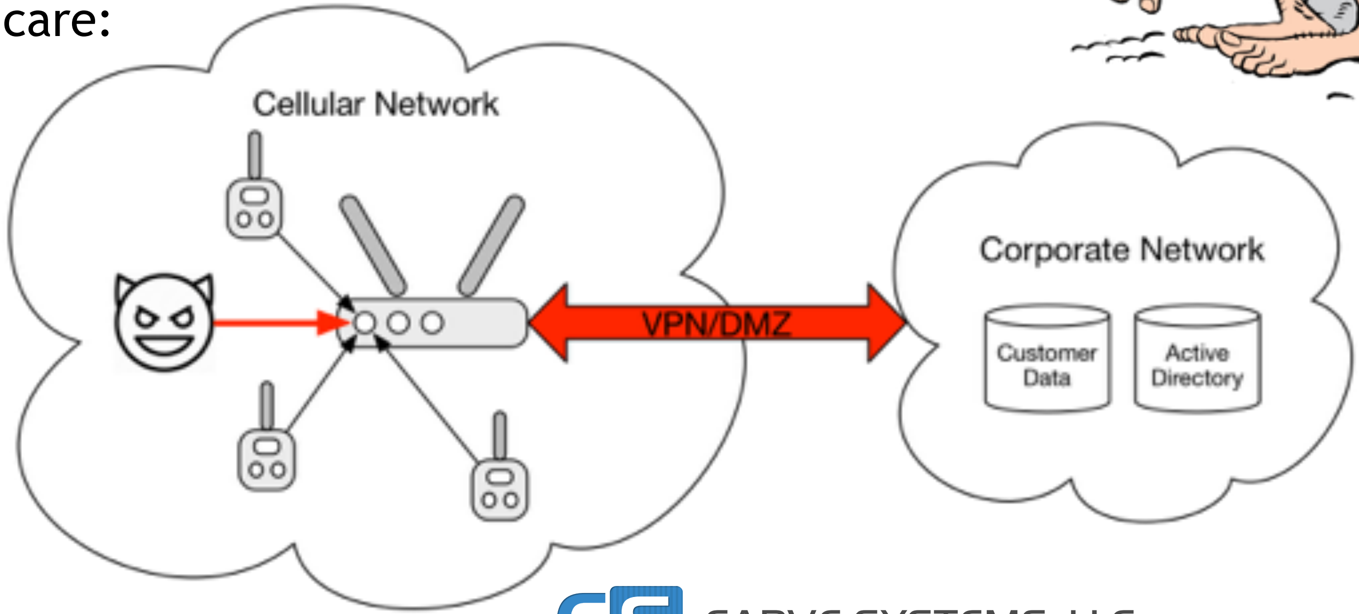
- We’ll see shellshock until the end of time.

*http://blog.talosintel.com/2016/02/trane-iot.html

Why do you care?

Don't care:

Do care:



What to do (Enterprise)

- Network Strategy
  - Keep devices off the corporate network (when possible), and off the Internet
- Threat Model your devices
  - Physical access control is important
  - Ideally, before you buy them
  - If important enough, perform a pen test
- Uniformity of data makes anomaly detection easier
  - Quieter control networks make it easier to tune IDS

What to do (Devices)

- Eliminate bad trust relationships: what I do has no effect on others
- Patch bugs! Lots of software re-use
- Fail closed
- Secure defaults
- Implement the 80% hardware security controls
- Don’t re-invent the wheel

Grog appears

{info,max,mike}@carvesystems.com
Twitter: @carvesystems, @msobell

Thank You, Organizers and Attendees!