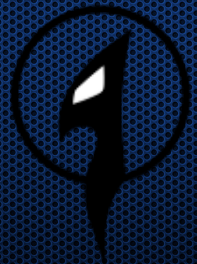
Responsible disclosure process

vulnerabilities of IP security cameras

“Kiberšahs 2016”
06.10.2016.



possible.lv

@KirilsSolovjovs
kirils.org

Me in a slide

- IT security expert; researcher at 1st Ltd, Latvia
- Skills: network flow analysis, reverse engineering, social engineering, penetration testing, security incident investigation, and the legal dimension of cyber security and cyber defence
- The responsible disclosure guy

How it all started

- Physical security looks like a hot topic…
- Let's teach physical security to people!
- Can we introduce some artificial weaknesses?
- Sure, **bring me a[ny] professional security camera**


Milesight

Before introducing weaknesses...

- It's usually a smart idea to check for pre-existing ones

Possible approaches

- It's all about the firmware:
  - connect to serial and dump it via bootloader
  - find it* online
    - a similar one will suffice
  - attack over the network

Likely result

Peace of mind replaced by additional worries:

- CVE-2016-2357
- CVE-2016-2356
- CVE-2016-2359
- CVE-2016-2358
- CVE-2016-2360

CVE-2016-2357

Milesight cameras contain hard-coded SSL private key

```
$ cd /etc/config
$ ls -la
total 8
drwxr-xr-x    2 root     root           304 May 12  2015 .
drwxr-xr-x   17 root     root          2976 Sep 26 23:34 ..
-rwxrwxrwx    1 root     root           944 Aug 29  2014 ssl_cert.pem
-rwxrwxrwx    1 root     root           887 Aug 29  2014 ssl_key.pem
$ md5sum *
676f33a8a7db627d01c4cd5951a15510  ssl_cert.pem
0ffeadb14227aab171ede207bf21adee  ssl_key.pem
```

CVE-2016-2356

Milesight cameras vulnerable to buffer overflow of username/password fields in CGI bin

- Requesting a CGI script crashes the webserver if the combined length of HTTP username and HTTP password is more than 31 symbols
- Indicative of a buffer overflow

CVE-2016-2359

Milesight cameras do not properly authenticate commands submitted to CGI bin

- Requesting a privileged action simultaniosuly with an unprivileged one over vb.htm leads to both actions being executed without authorization

CVE-2016-2358

Milesight cameras contain hard-coded default credentials

- If there are less than the maximum of 10 users configured, attacker can use any of the empty users to access the camera over HTTP
- Empty users' authority set to 0 (full access)
- There is a check built in JavaScript that *prevents* this from actually working via the web interface

CVE-2016-2360

Milesight cameras use a vulnerable version of dropbear with hard-coded default credentials

- Dropbear sshd v0.53.1 has multiple publicly known vulnerabilities
- Root password is set to a shared default value for all cameras

```
# head -c16 /etc/shadow
root:$1$acQMceF9
```


DEMO DEMO DEMO

Milesight's response

- +10w: "I have forwarded your information to the appropriate party. If there is an interest, someone will contact you."
    - IF?!? Seriously?
- +36w: “Fix will be issued in 2 weeks”
- +40w: “We will have fix ready by the end of the month…”
- +45w: “We have fixed it!”

All fixed now (+49w)

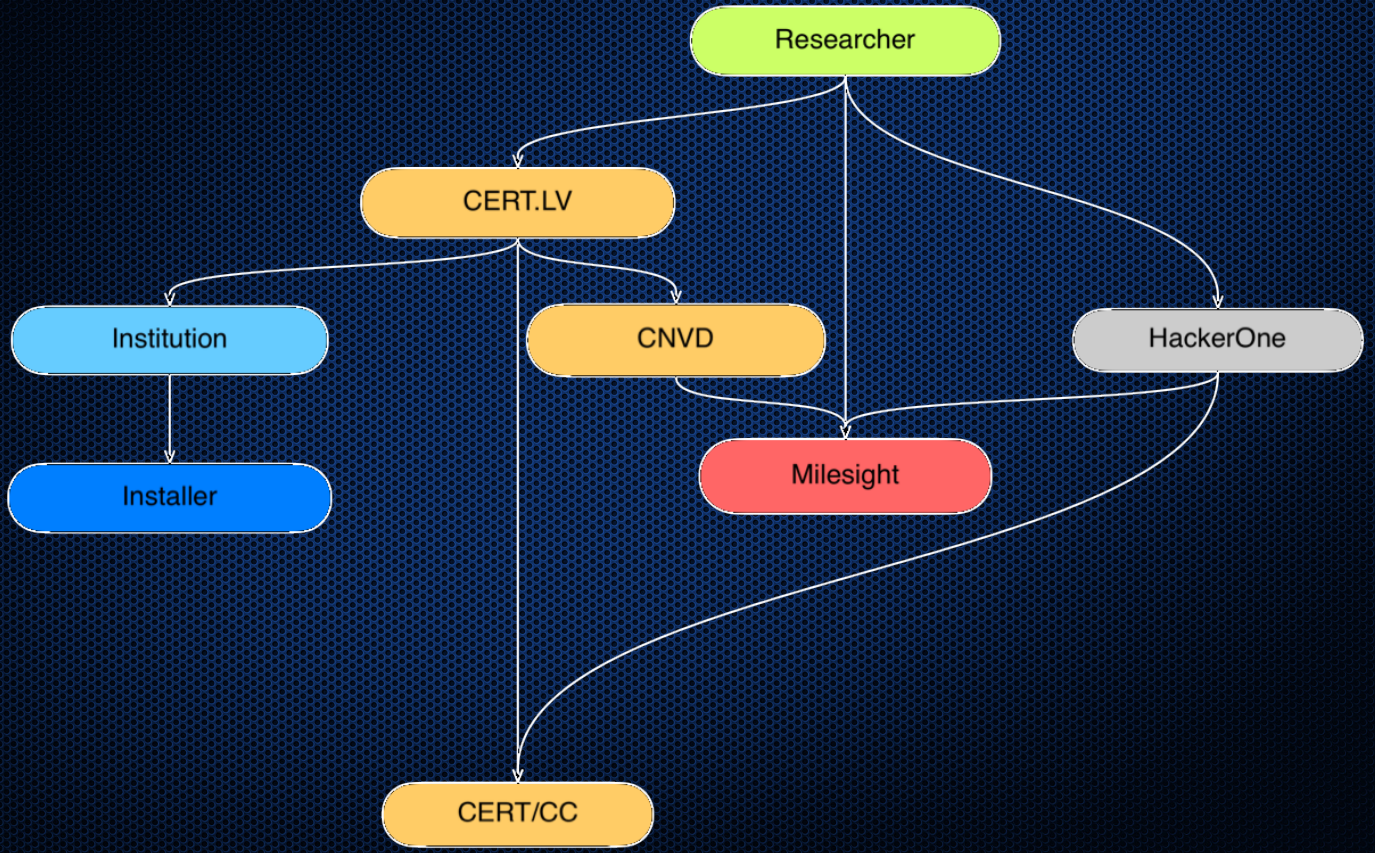
Firmware

Please Contact Us

support.milesight

support@milesight.com

Organisations involved



Lessons learned

- Time to locate five vulnerabilities – less than 24 hours
- Time to get them fixed – 48 weeks (and counting?)
- Actual responsible disclosure can get quite messy and complex
- Lack of clear contact points is a challenge to responsible disclosure

Recommendations for security officers

- Brace yourselves – reports are coming!
  - Be ready to process RDP reports, even if you haven't published a policy
  - Better yet publish a policy!
- Think about incentives – what could motivate a hacker to go to you rather to a grey market vendor?
  - Hint: maybe a streamlined process?
- Convince your CFO that investing in cyber security is worth it

Recommendations for policy makers

- Ensure that efficient cooperation platform is available for working with actors outside of EU
  - Promote shared values
- Establish clear contact points and governmental brokers
- Require cyber safety for all relevant products not unlike:
  - food
  - cars
  - electronics

Thank you for your time!