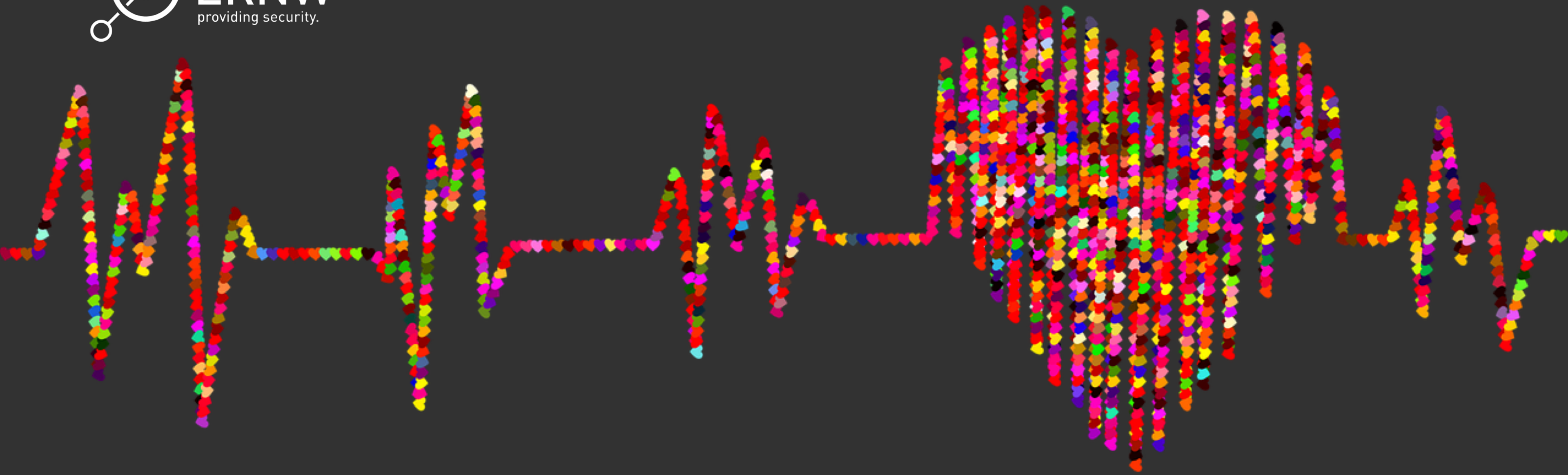


Medical Device Security: Please (don‘t) be patient!

Julian Suleder, jsuleder@ernw.de

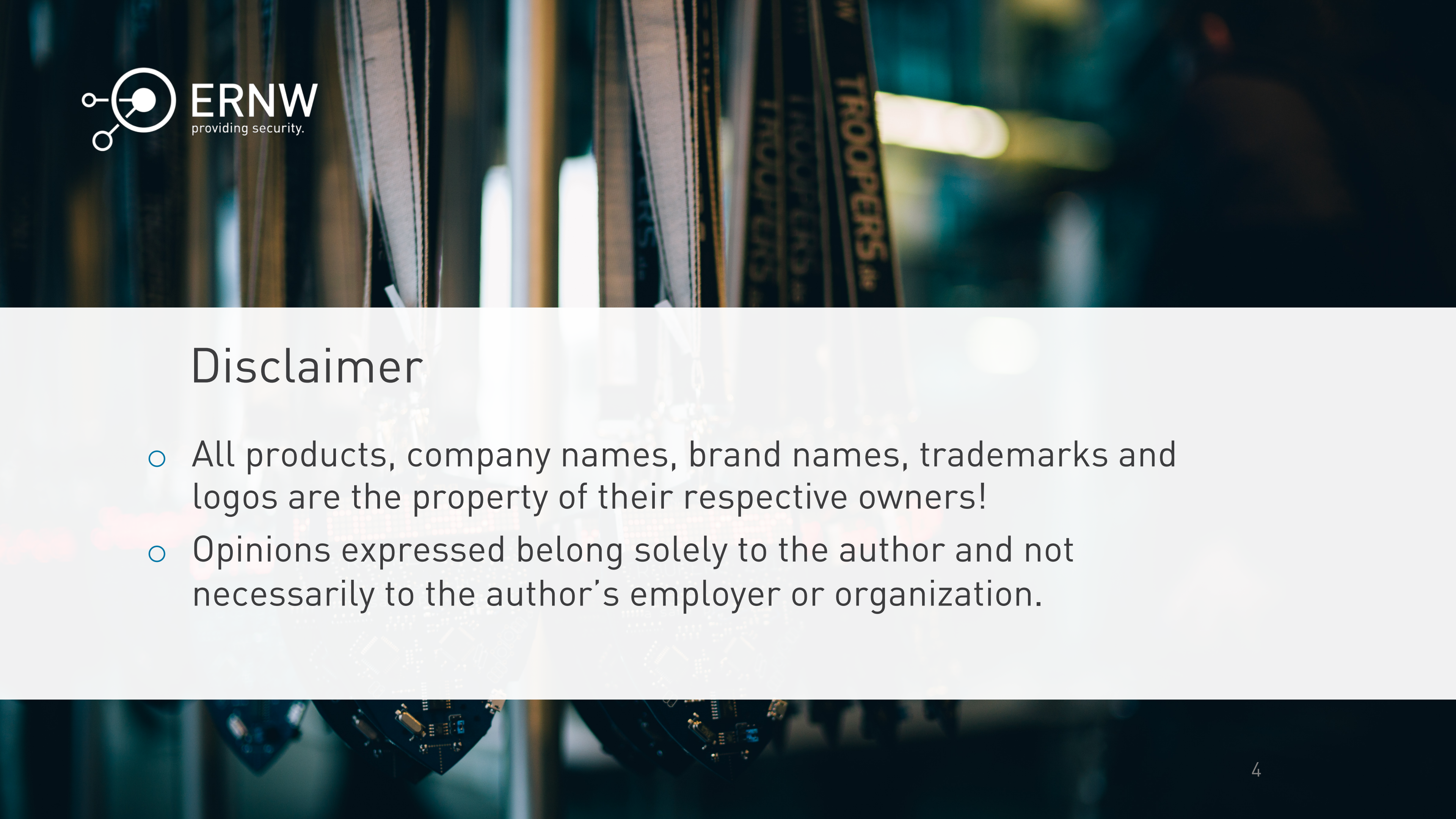
ERNW
RESEARCH
pursuing knowledge.

Who Am I

- M.Sc. & B.Sc. Medical Informatics
  - Heidelberg & Heilbronn University
  - Master Thesis @ DKFZ Heidelberg
  - Teaching: IT-Security Lab @ Heilbronn University
- SIG Consumer Health Informatics (CHI), GMDS e.V.
- Security Analyst & Researcher @ ERNW Research
- Twitter: @jsuleder

Agenda

- Anamnesis:
  - The State of IT Security in healthcare
  - Medical device regulations
- Diagnostics:
  - Examples of insecure medical devices
- Therapy:
  - Recommendations
  - Outlook & Future Research



Disclaimer

- All products, company names, brand names, trademarks and logos are the property of their respective owners!
- Opinions expressed belong solely to the author and not necessarily to the author’s employer or organization.

Image by marionbrun on Pixabay

Anamnesis

The Environment

The Environment – Health Delivery Organizations (HDO)

- Highly-specialized, not comparable to industry environments
- Various audiences with individual backgrounds, expectations and needs
- Continuously changing IT systems landscape
- Business processes are to be digitized
- Financial pressure
- Operations is key

Image by mohamed_hassan on Pixabay

The perfect target?

- HDOs rely on digital health records to provide their health services
- Healthcare is behind other industries in protecting its infrastructure:
  - Outdated technology
  - Insecure network-enabled medical devices
  - Adoption of digital patient records
  - Manufacturers push security problems to the provider

Photo by Annie Spratt on Unsplash

ERNW RESEARCH pursuing knowledge.

NHS 2017: WannaCry

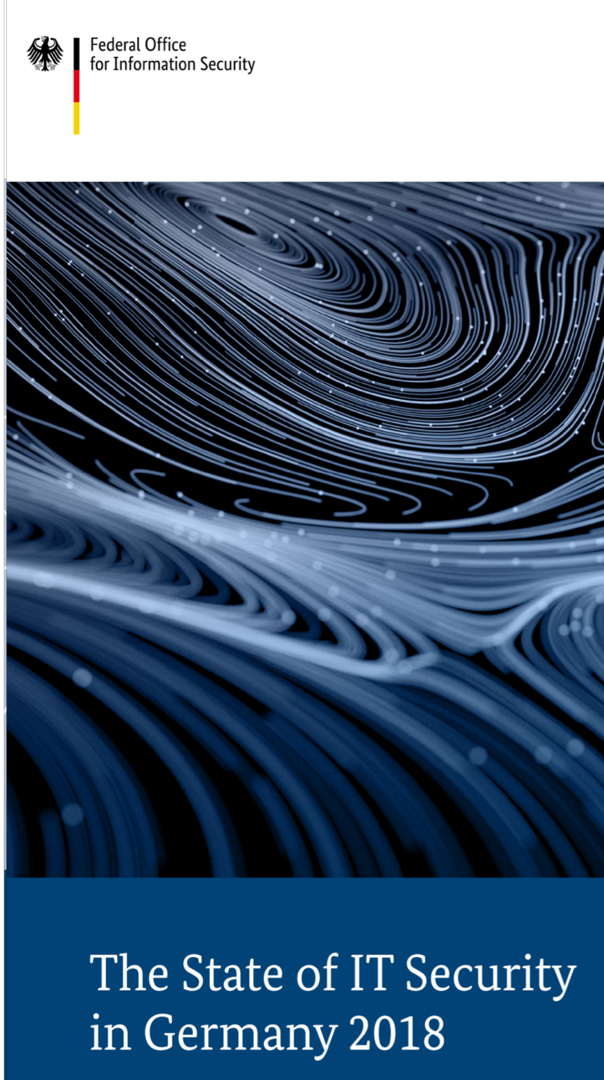
- Vor dem Vorfall:
  - Security Assessment von 88/236 NHS Trusts
  - Keine einzige hat bestanden
- Auswirkungen
  - Störung in mindestens 34% der Trusts in England
  - 1.220 infizierte Diagnosegeräte
  - Geräte wurden entweder infiziert oder isoliert
  - 6.912 abgesagte Termine
  - 139 dringende Überweisungen für potenzielle Krebserkrankungen abgesagt

Photo by Annie Spratt on Unsplash

The State of IT Security in Germany

- Federal Office for Information Security (BSI)
- 2018:
  - More smart devices marketed every year
  - Attacks with potential threats to patient safety increase
  - Key Observations:
    - Missing or weak authentication mechanisms
    - Weak or no encryption used to communicate and store data
  - Operation is key: Medical functionality vs. Security

[https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html, 2019-02-19]

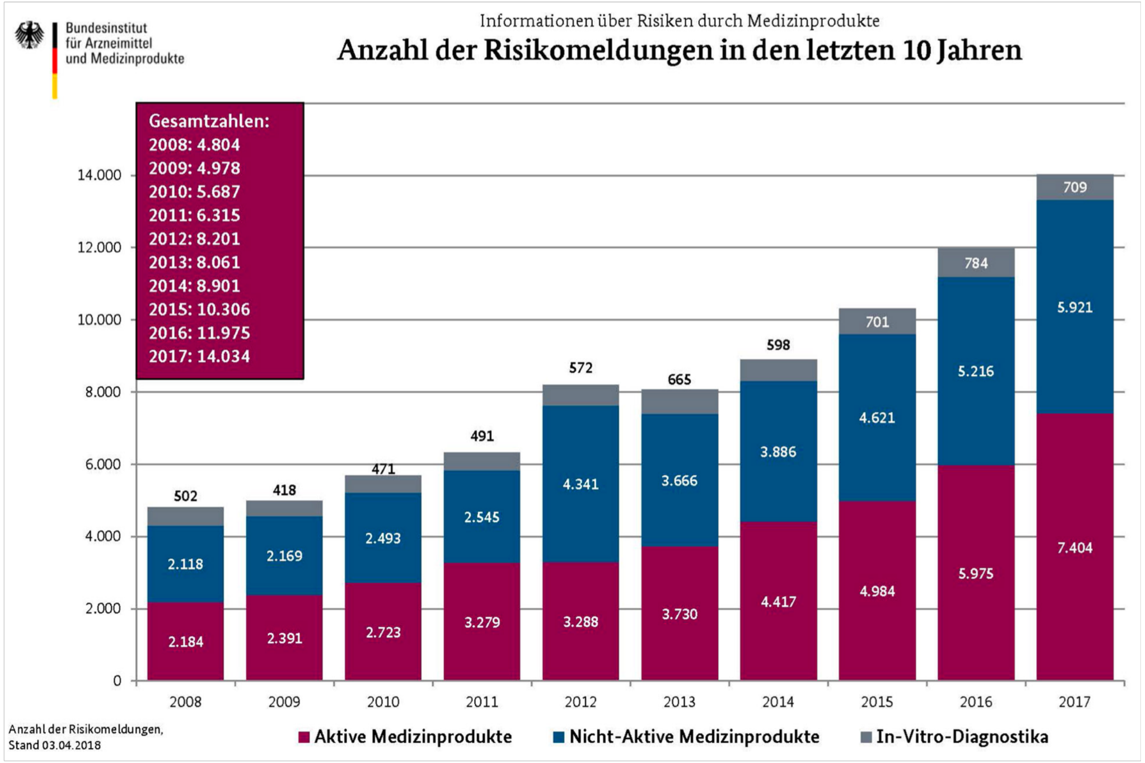


Federal Office for Information Security

The State of IT Security in Germany 2018

Statistics provided by the BfArM

- Risk reports increase
- 2017: 20 reports/day
- Bias:
  - Changes in the environment?
  - More in-depth investigations?
  - Awareness to report?



Bundesinstitut für Arzneimittel und Medizinprodukte

Informationen über Risiken durch Medizinprodukte

Anzahl der Risikomeldungen in den letzten 10 Jahren

Anzahl der Risikomeldungen, Stand 03.04.2018

[https://www.bfarm.de/DE/Service/Statistiken/MP_statistik/AllgStatAngaben/Anzahl-Risikomeldungen/_node.html, 2019-03-10]

Anamensis

Medical Device Regulations

Medical Device Classification

- In the European Economic Area directives and legal regulations classify medical products
  - Depending on their intended use (primary)
  - Possible harms to patients (secondary)
- Depending on the classification MDMs must:
  - Implement processes for quality/risk management, SDL and usability for products including software

Photo by rawpixel on Unsplash

What is a medical device?

- Basically everything intended by the manufacturer to be used for human beings for the purpose of:
  - diagnosis, prevention, monitoring, treatment or alleviation of disease,
  - diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
  - investigation, replacement or modification of the anatomy or of a physiological process,
  - control of conception

See: Council Directive 93/42/EEC of 14 June 1993 concerning medical devices

ERNW RESEARCH pursuing knowledge.

Mobile Apps & Fitness Trackers

- Apps that meet the definition of a medical device are considered SaMD
- Future developments of health apps and fitness trackers may show how this will affect certification requirements
- Apple introduced health records in iOS (US)
- Apps for the Apple Watch Series 4 with ECG sensor will get FDA certification

Apple Watch Apps:

- DEN180042
- DEN180044

Photo by rawpixel on Unsplash

Medical Device Regulation (MDR) – 2020/05

- Supersedes EU- and most nation-specific legal regulations
- Implications:
    - More controls for the identification and tracking of defective devices
    - More critical classification of medical devices and SaMD
    - Demands much more effort on software design, software lifecycle processes and risk management

Effective since May, 25 2017!

Medical Device Regulation (MDR) – 2020/05

- Supersedes EU- and most nation-specific legal regulations
- Implications:
  - More controls for the identification and tracking of defective devices
  - More critical classification of medical devices and SaMD
  - Demands much more effort on software design, software lifecycle processes and risk management

ERNW
providing security.

Photo by Sara Bakhshi on Unsplash

Diagnostics

Examples of insecure Medical Devices

Defects in Medical Devices

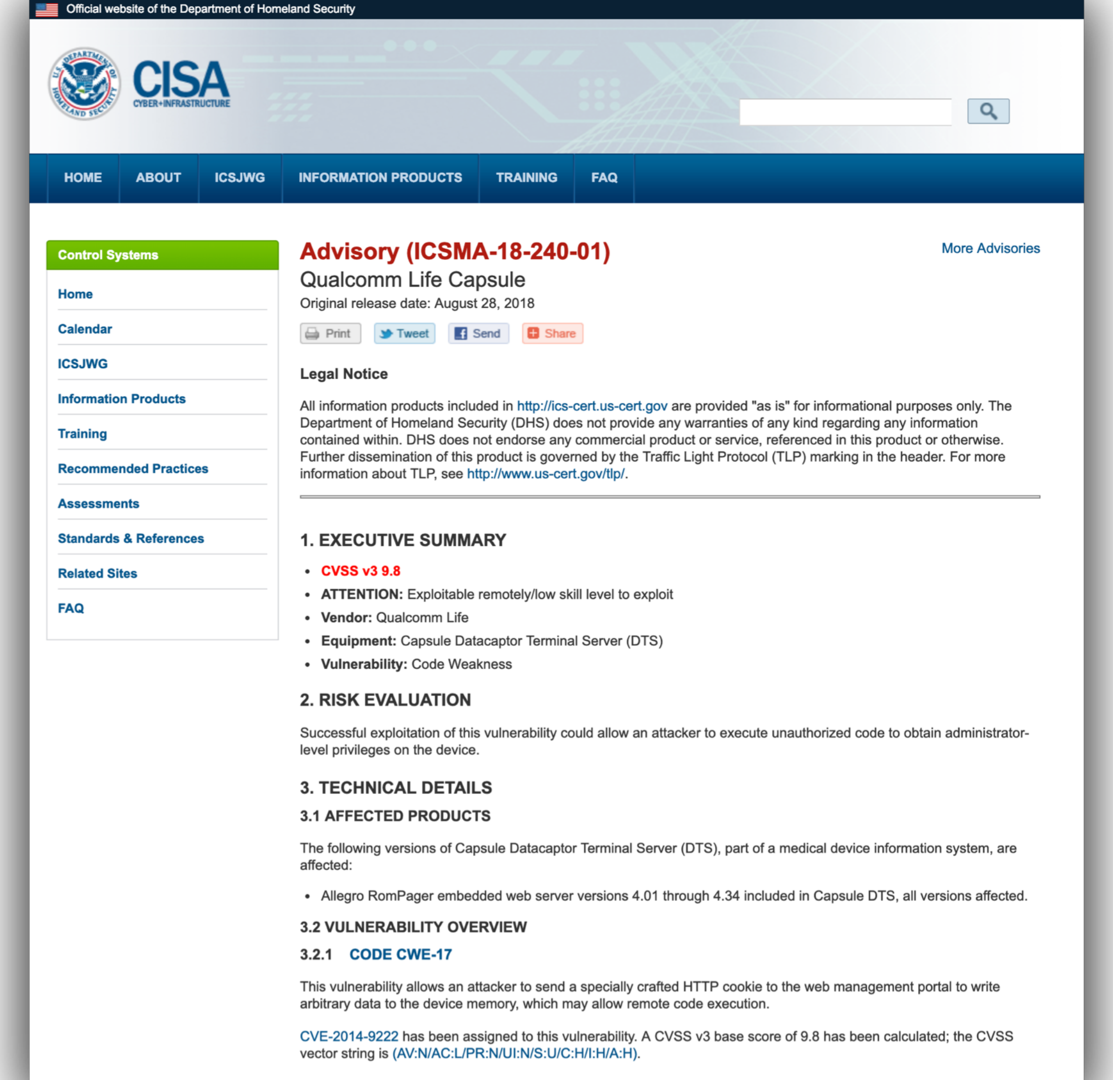
- Vulnerabilities in healthcare are sensitive
- Disclosures should be very well thought-out and coordinated → may expose patients to risks
- A concealment of vulnerabilities and incidents means that those affected cannot themselves estimate the risk
- There should be a public chronology in which all measures are documented in a transparent way

Where to get information from?

- Named authorities ensure the central analysis and evaluation of risks arising from medical devices
  - Germany: Federal Institute for Drugs and Medical Devices (BfArM)
  - US: Food and Drug Administration (FDA)
- Incidents and risks must be reported by users and manufacturers
  - Incidents that have led, or could have led to the death or serious deterioration in the state of health of a patient or another person <u>must be reported</u>

Where to get information from?

- No manufacturer is going voluntarily endanger his market situation
- The ICS-CERT (USA) publishes detailed advisories:
  - Explanation of the vulnerabilities, incl. CVE, severity rating, ...
  - Section of mitigations and recommendations by the ICS-CERT
  - Measures taken by the manufacturer
  - https://ics-cert.us-cert.gov/advisories (search for ICSMA)
- **Since 2018**: German authorities try to actively improve the situation with recommendations for MDMs, funded research, ...



Advisory (ICSMA-18-240-01)

Qualcomm Life Capsule

Original release date: August 28, 2018

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Qualcomm Life
- **Equipment:** Capsule Datacaptor Terminal Server (DTS)
- **Vulnerability:** Code Weakness

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to execute unauthorized code to obtain administrator-level privileges on the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Capsule Datacaptor Terminal Server (DTS), part of a medical device information system, are affected:

- Allegro RomPager embedded web server versions 4.01 through 4.34 included in Capsule DTS, all versions affected.

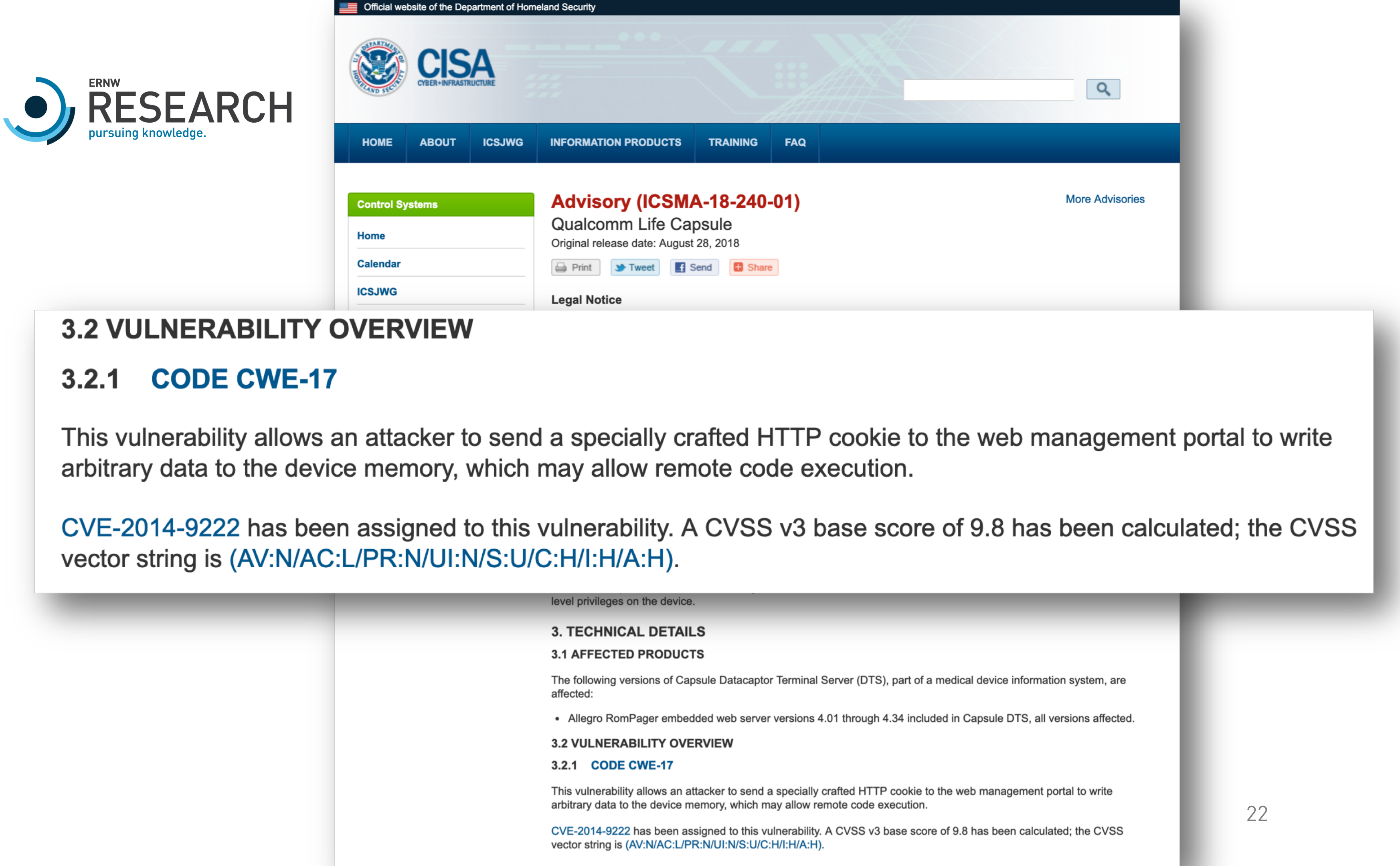
3.2 VULNERABILITY OVERVIEW

3.2.1 CODE CWE-17

This vulnerability allows an attacker to send a specially crafted HTTP cookie to the web management portal to write arbitrary data to the device memory, which may allow remote code execution.

CVE-2014-9222 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

https://ics-cert.us-cert.gov/advisories/ICSMA-18-240-01



Advisory (ICSMA-18-240-01)

Qualcomm Life Capsule

Original release date: August 28, 2018

Legal Notice

3.2 VULNERABILITY OVERVIEW

3.2.1 CODE CWE-17

This vulnerability allows an attacker to send a specially crafted HTTP cookie to the web management portal to write arbitrary data to the device memory, which may allow remote code execution.

CVE-2014-9222 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

level privileges on the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Capsule Datacaptor Terminal Server (DTS), part of a medical device information system, are affected:

- Allegro RomPager embedded web server versions 4.01 through 4.34 included in Capsule DTS, all versions affected.

3.2 VULNERABILITY OVERVIEW

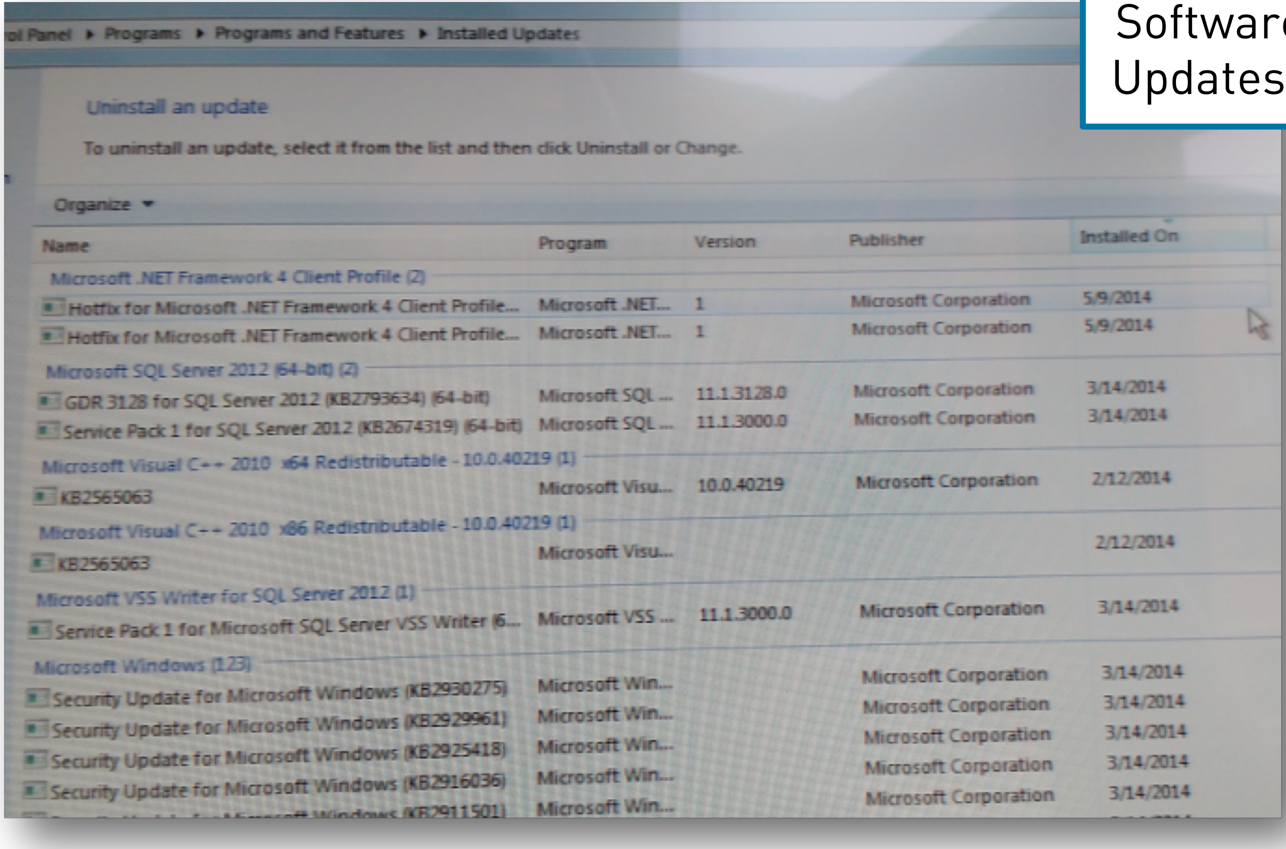
3.2.1 CODE CWE-17

This vulnerability allows an attacker to send a specially crafted HTTP cookie to the web management portal to write arbitrary data to the device memory, which may allow remote code execution.

CVE-2014-9222 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

https://ics-cert.us-cert.gov/advisories/ICSMA-18-240-01

Target: Endoscope (2017)



ol Panel ▸ Programs ▸ Programs and Features ▸ Installed Updates

Uninstall an update

To uninstall an update, select it from the list and then click Uninstall or Change.

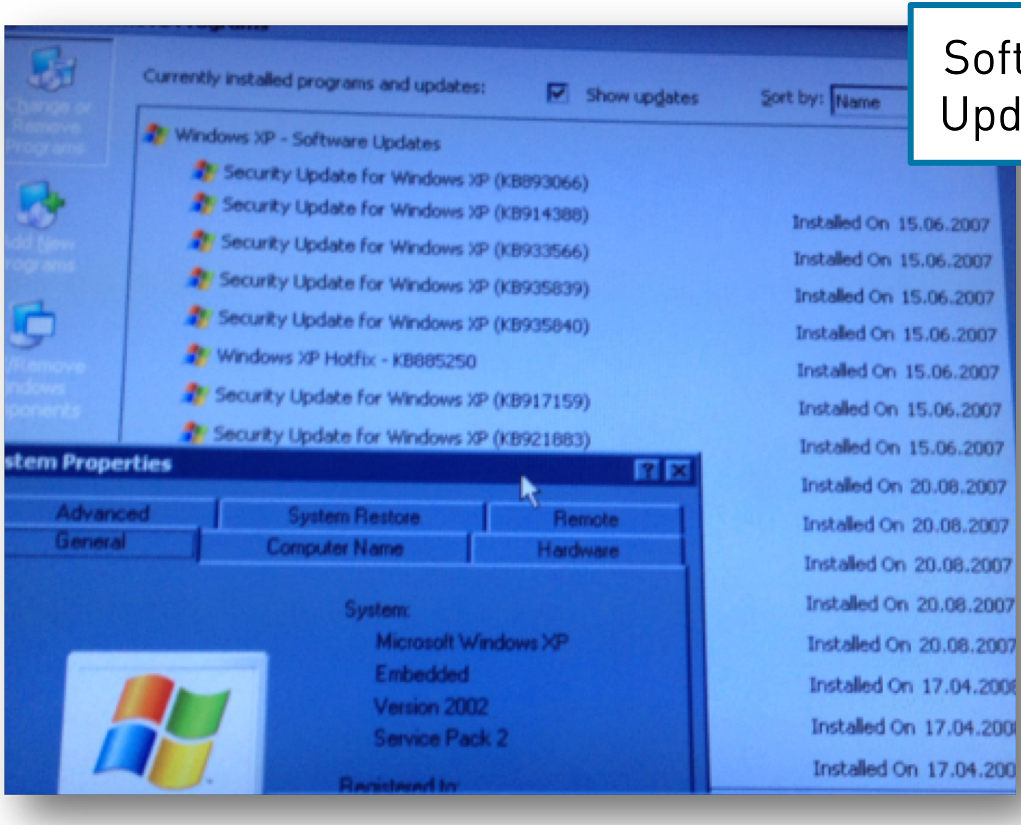
Organize ▾

Name	Program	Version	Publisher	Installed On
Microsoft .NET Framework 4 Client Profile (2)				
Hotfix for Microsoft .NET Framework 4 Client Profile...	Microsoft .NET...	1	Microsoft Corporation	5/9/2014
Hotfix for Microsoft .NET Framework 4 Client Profile...	Microsoft .NET...	1	Microsoft Corporation	5/9/2014
Microsoft SQL Server 2012 (64-bit) (2)				
GDR 3128 for SQL Server 2012 (KB2793634) (64-bit)	Microsoft SQL ...	11.1.3128.0	Microsoft Corporation	3/14/2014
Service Pack 1 for SQL Server 2012 (KB2674319) (64-bit)	Microsoft SQL ...	11.1.3000.0	Microsoft Corporation	3/14/2014
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 (1)				
KB2565063	Microsoft Visu...	10.0.40219	Microsoft Corporation	2/12/2014
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (1)				
KB2565063	Microsoft Visu...			2/12/2014
Microsoft VSS Writer for SQL Server 2012 (1)				
Service Pack 1 for Microsoft SQL Server VSS Writer (6...	Microsoft VSS ...	11.1.3000.0	Microsoft Corporation	3/14/2014
Microsoft Windows (123)				
Security Update for Microsoft Windows (KB2930275)	Microsoft Win...		Microsoft Corporation	3/14/2014
Security Update for Microsoft Windows (KB2929961)	Microsoft Win...		Microsoft Corporation	3/14/2014
Security Update for Microsoft Windows (KB2925418)	Microsoft Win...		Microsoft Corporation	3/14/2014
Security Update for Microsoft Windows (KB2916036)	Microsoft Win...		Microsoft Corporation	3/14/2014
Security Update for Microsoft Windows (KB2911501)	Microsoft Win...			

Software Updates?

ERNW RESEARCH pursuing knowledge.

Target: Ultrasound Scanner (2017)



Change or Remove Programs

dd New rograms

/Remove indows ponents

Currently installed programs and updates: ☑ Show updates Sort by: Name

Windows XP - Software Updates

Security Update for Windows XP (KB893066)

Security Update for Windows XP (KB914388)

Security Update for Windows XP (KB933566)

Security Update for Windows XP (KB935839)

Security Update for Windows XP (KB935840)

Windows XP Hotfix - KB885250

Security Update for Windows XP (KB917159)

Security Update for Windows XP (KB921883)

Installed On 15.06.2007

Installed On 15.06.2007

Installed On 15.06.2007

Installed On 15.06.2007

Installed On 15.06.2007

Installed On 15.06.2007

Installed On 15.06.2007

Installed On 20.08.2007

Installed On 20.08.2007

Installed On 20.08.2007

Installed On 20.08.2007

Installed On 20.08.2007

Installed On 17.04.200

Installed On 17.04.200

Installed On 17.04.200

stem Properties

System:

Microsoft Windows XP

Embedded

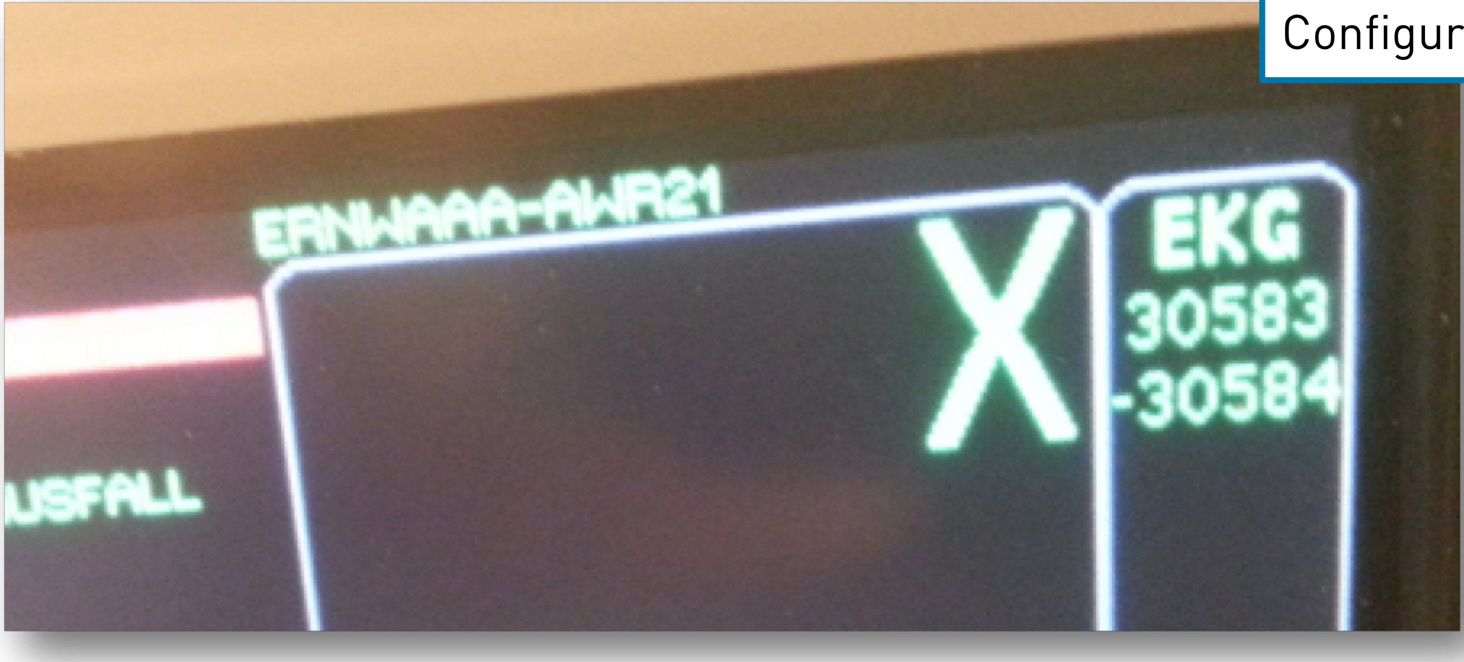
Version 2002

Service Pack 2

Registered to:

Software Updates?

Target: Patient Monitor



Unreasonable Configuration!

Photo by Owen Beard on Unsplash

Target: Image Management System

- Most run on Windows 7 workstations with "special" user account
- Updates intensively tested by manufacturers → delays
- Vulnerability: Logging domain authentication credentials
  - Unauthorized access to sensitive information such as
    - Health information
    - Modify device configurations
    - Attack secondary systems
- Prerequisites: User privileges on the OS
  - Credentials on post-it on screen
  - Remote access using an unpatched vulnerability…

Target: Infusion Pump

- Moved on demand within the hospital
- Intravenous delivery of nutrients or medications
- Often controlled by a central managing software in the hospital wireless or wired LAN
- Receive drug libraries, software updates, pump commands and configuration data over the network

Unauthenticated open Port 23/Telnet

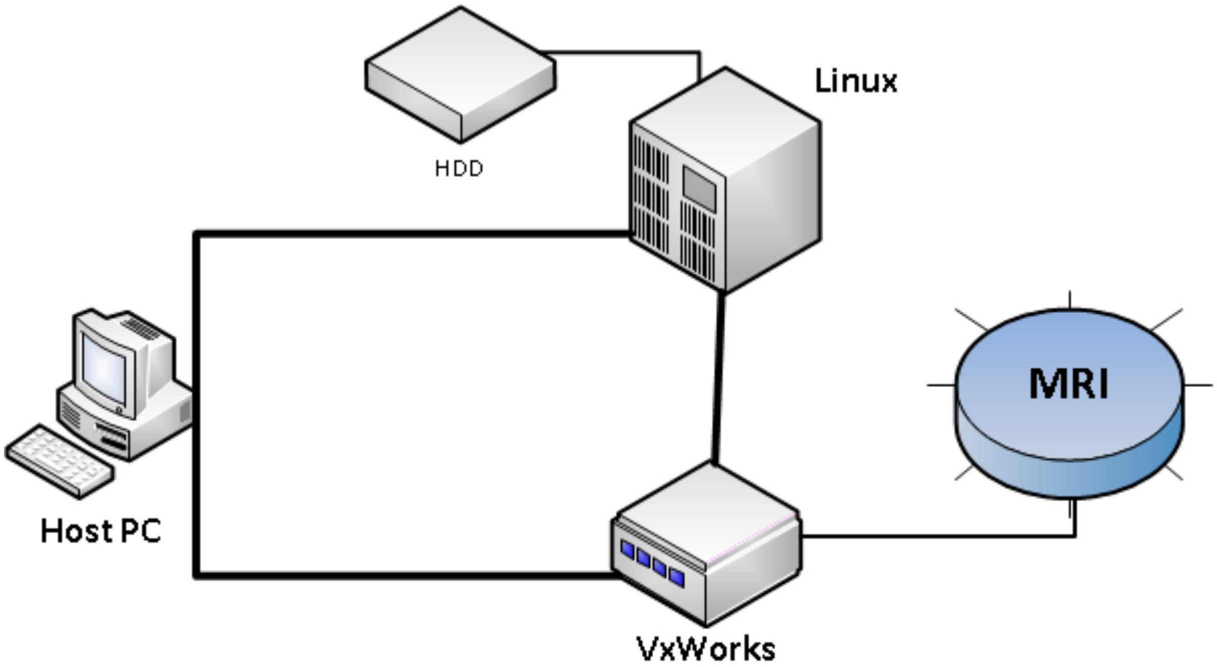
- Root privileges on Port 23/TELNET (user: `root`, pw: `<empty>`)
- Can be discovered by a low-skilled attacker
- Prerequisites: Access to device's network using e.g. bedside LAN sockets
- Having different LAN sockets for entertainment systems and medical devices does not limit the access
- All the pumps are in the same (flat) managing network
  - An attacker will discover all pumps

[https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B, 2019-03-10]

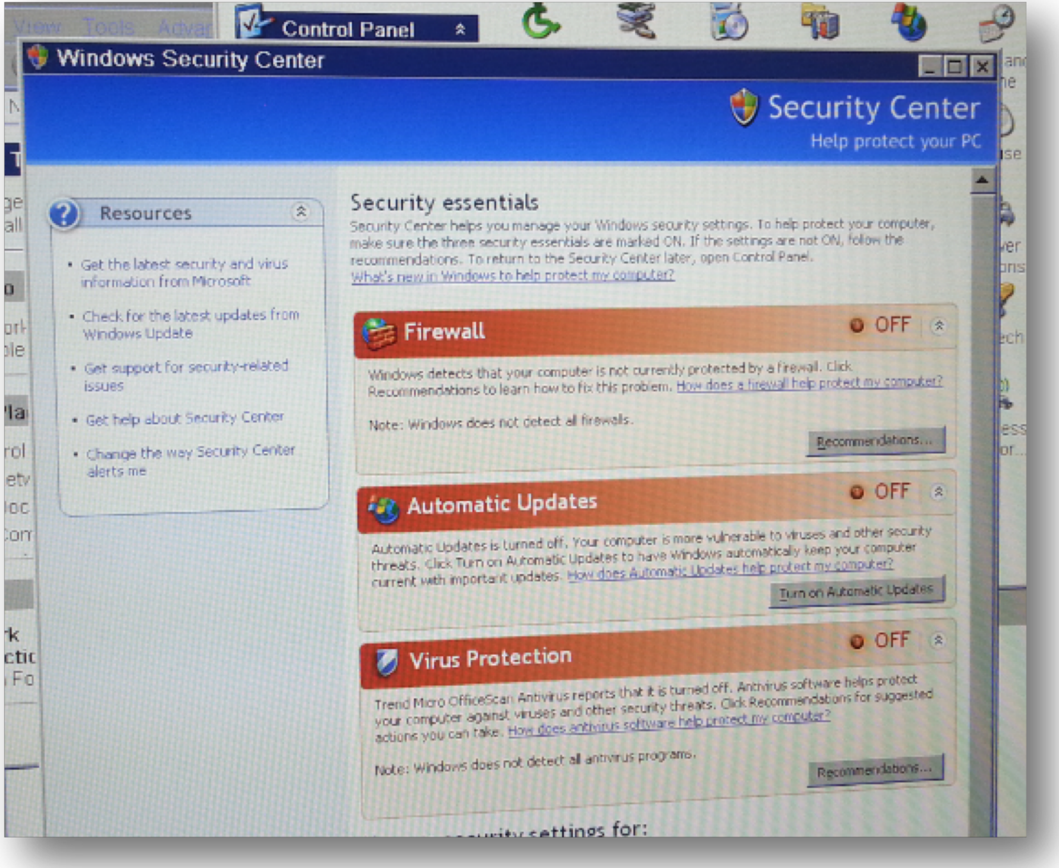
Target: Magnetic resonance imaging (MRI)

Really cool! ☺

Target: Magnetic resonance imaging (MRI)



Target: Magnetic resonance imaging (MRI)



- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Firewall: OFF

Windows detects that your computer is not currently protected by a firewall. Click Recommendations to learn how to fix this problem. How does a firewall help protect my computer?

Note: Windows does not detect all firewalls.

Automatic Updates: OFF

Automatic Updates is turned off. Your computer is more vulnerable to viruses and other security threats. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates. How does Automatic Updates help protect my computer?

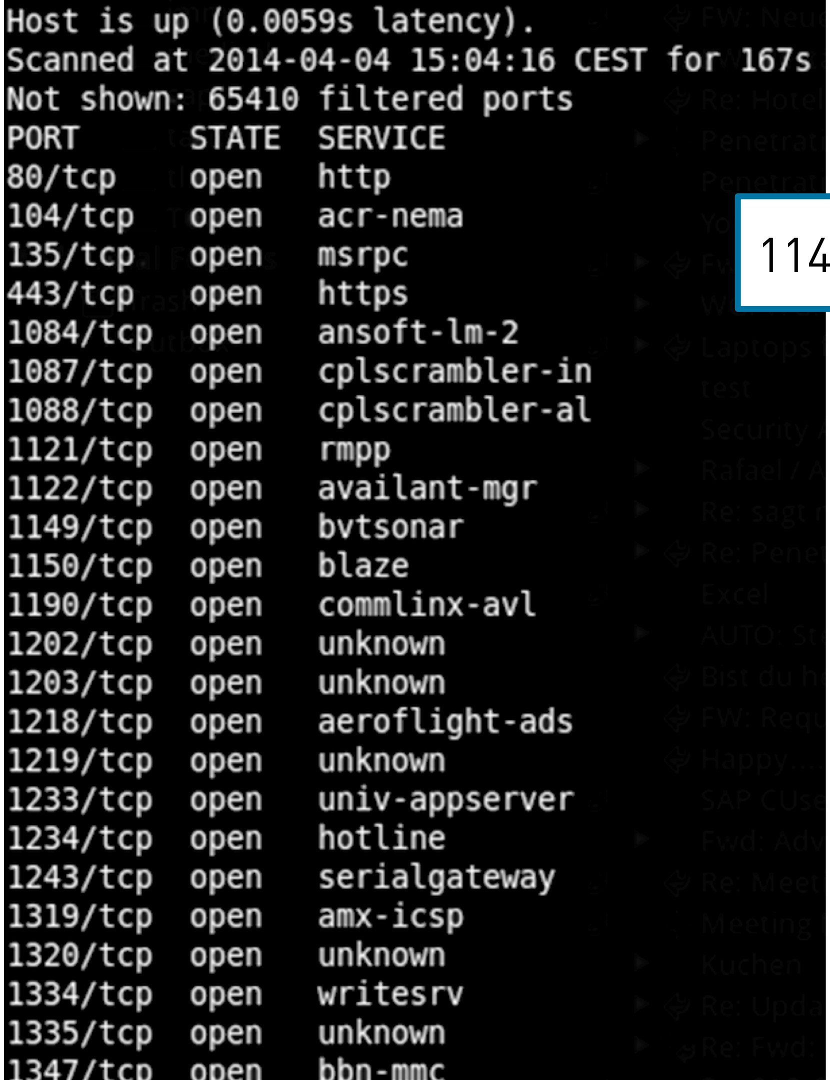
Virus Protection: OFF

Trend Micro OfficeScan Antivirus reports that it is turned off. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

curity settings for:

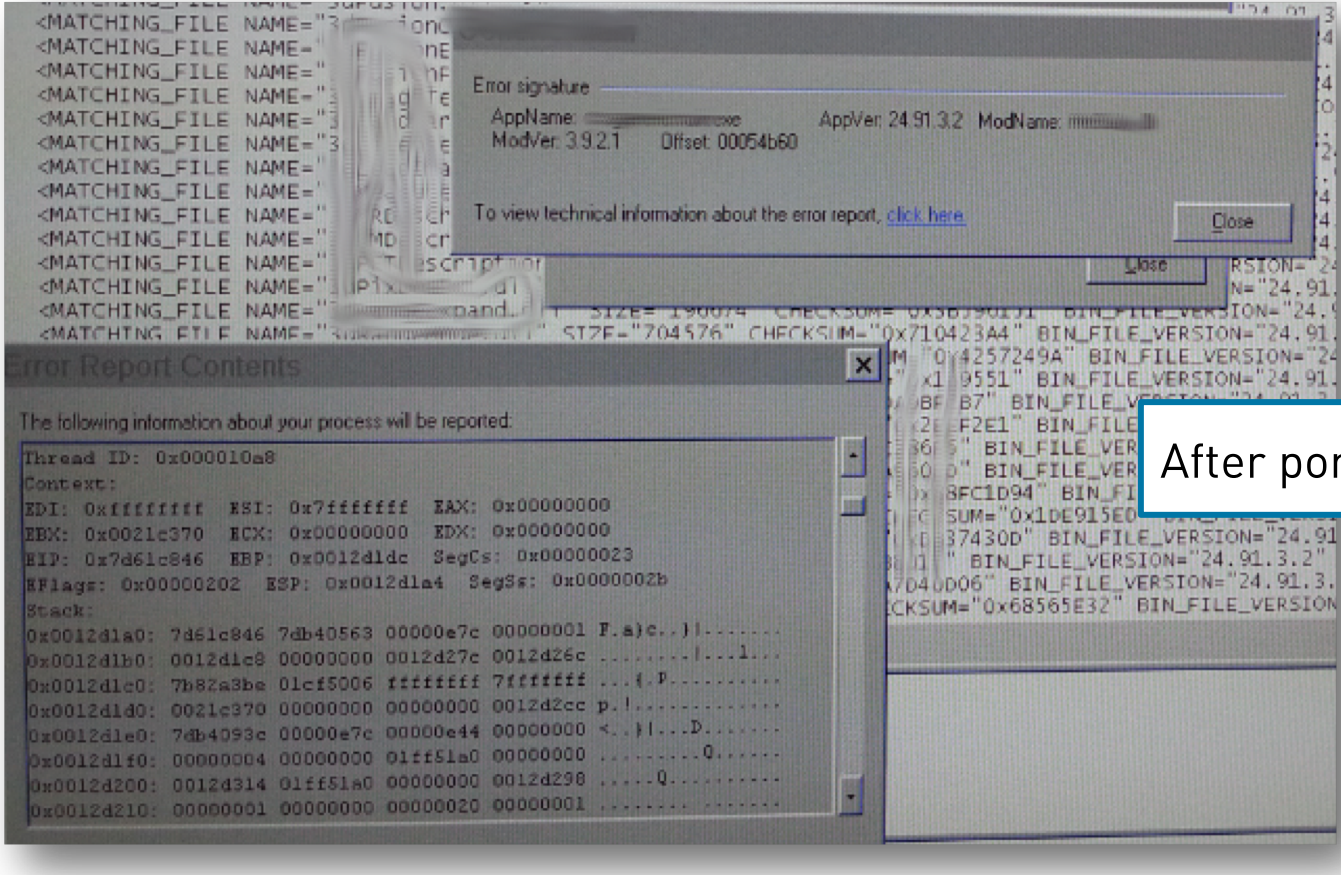
Host system...



```
Host is up (0.0059s latency).
Scanned at 2014-04-04 15:04:16 CEST for 167s
Not shown: 65410 filtered ports
PORT      STATE  SERVICE
80/tcp    open   http
104/tcp   open   acr-nema
135/tcp   open   msrpc
443/tcp   open   https
1084/tcp  open   ansoft-lm-2
1087/tcp  open   cplscrambler-in
1088/tcp  open   cplscrambler-al
1121/tcp  open   rmpp
1122/tcp  open   availant-mgr
1149/tcp  open   bvtsonar
1150/tcp  open   blaze
1190/tcp  open   commlinx-avl
1202/tcp  open   unknown
1203/tcp  open   unknown
1218/tcp  open   aeroflight-ads
1219/tcp  open   unknown
1233/tcp  open   univ-appserver
1234/tcp  open   hotline
1243/tcp  open   serialgateway
1319/tcp  open   amx-icsp
1320/tcp  open   unknown
1334/tcp  open   writesrv
1335/tcp  open   unknown
1347/tcp  open   bbn-mmc
```

114 Open Ports...

Target: Magnetic resonance imaging (MRI)



```
<MATCHING_FILE NAME="3[redacted]onc
<MATCHING_FILE NAME="[redacted]nE
<MATCHING_FILE NAME="[redacted]nF
<MATCHING_FILE NAME="3[redacted]g Te
<MATCHING_FILE NAME="3[redacted]d r
<MATCHING_FILE NAME="3[redacted]e
<MATCHING_FILE NAME="[redacted]a
<MATCHING_FILE NAME="[redacted]E
<MATCHING_FILE NAME="[redacted]RD Sch
<MATCHING_FILE NAME="[redacted]MD Scr
<MATCHING_FILE NAME="[redacted]escription
<MATCHING_FILE NAME="[redacted]Pix[redacted]dl
<MATCHING_FILE NAME="[redacted]pand.
<MATCHING_FILE NAME="3[redacted]" SIZE="704576" CHECKSUM="0x710423A4" BIN_FILE_VERSION="24.91.
                                                   M "0x4257249A" BIN_FILE_VERSION="24
                                                   " x1 9551" BIN_FILE_VERSION="24.91.
                                                   BF B7" BIN_FILE_V
                                                   2E F2E1" BIN_FILE
                                                   36 5" BIN_FILE_VER
                                                   60 D" BIN_FILE_VER
                                                   0x 8FC1D94" BIN_FI
                                                   SUM="0x1DE915E0
                                                   37430D" BIN_FILE_VERSION="24.91
                                                   " BIN_FILE_VERSION="24.91.3.2"
                                                   A7D40D06" BIN_FILE_VERSION="24.91.3.
                                                   CKSUM="0x68565E32" BIN_FILE_VERSION
```

Error signature

AppName: [redacted].exe   AppVer: 24.91.3.2   ModName: [redacted]
ModVer: 3.9.2.1   Offset: 00054b60

To view technical information about the error report, click here.

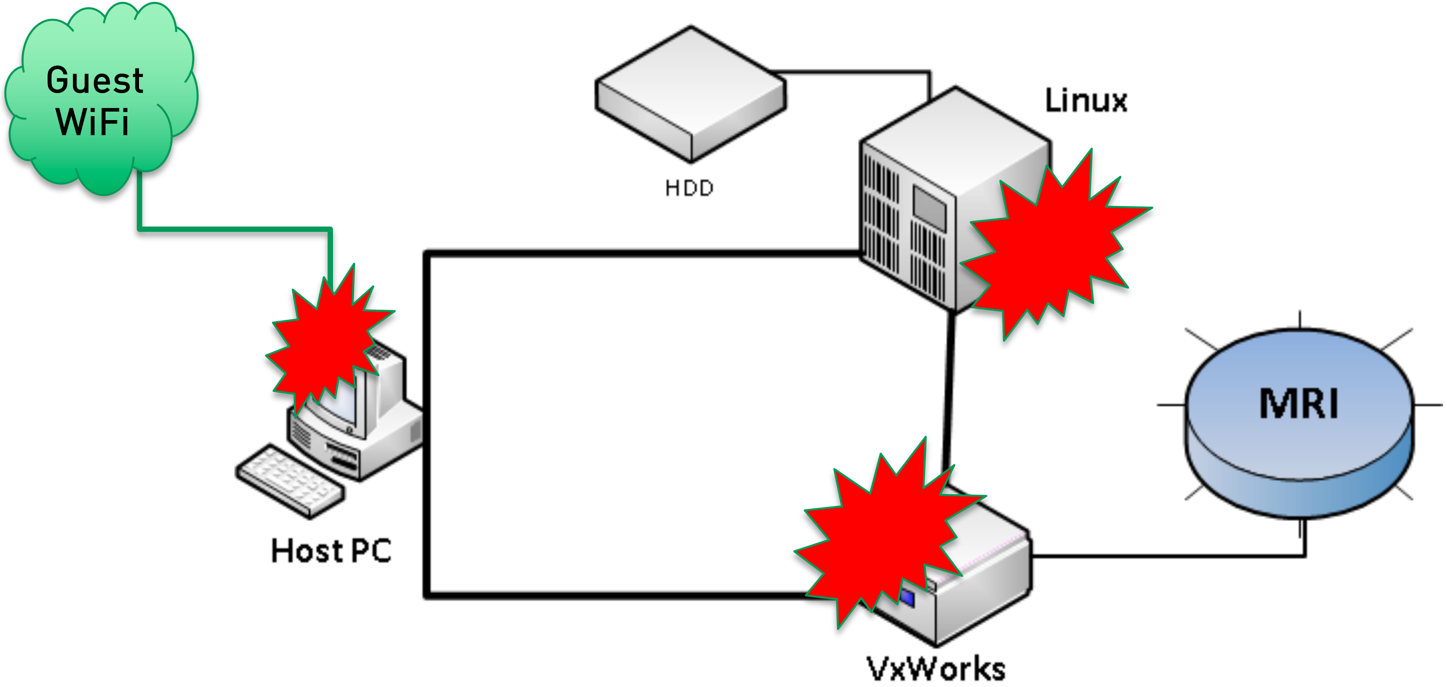
Error Report Contents

The following information about your process will be reported:

```
Thread ID: 0x000010a8
Context:
EDI: 0xffffffff  ESI: 0x7fffffff  EAX: 0x00000000
EBX: 0x0021c370  ECX: 0x00000000  EDX: 0x00000000
EIP: 0x7d61c846  EBP: 0x0012d1dc  SegCs: 0x00000023
EFlags: 0x00000202  ESP: 0x0012d1a4  SegSs: 0x0000002b
Stack:
0x0012d1a0: 7d61c846 7db40563 00000e7c 00000001 F.a}c..}|.......
0x0012d1b0: 0012d1c8 00000000 0012d27c 0012d26c ........|...l...
0x0012d1c0: 7b82a3be 01cf5006 ffffffff 7fffffff ...{.P..........
0x0012d1d0: 0021c370 00000000 00000000 0012d2cc p.!.............
0x0012d1e0: 7db4093c 00000e7c 00000e44 00000000 <..}|...D.......
0x0012d1f0: 00000004 00000000 01ff51a0 00000000 ..........Q.....
0x0012d200: 0012d314 01ff51a0 00000000 0012d298 ......Q.........
0x0012d210: 00000001 00000000 00000020 00000001 ........ .......
```

After portscan...

Target: Magnetic resonance imaging (MRI)



Collection of manufacturer‘s statements

“We only need to make sure that there are proper authorization mechanisms.“

“… a hacker will always find a way …”

„We know that telnet is insecure, so we implemented a custom telnet command interpreter…“

“We don’t know what we are going to do with the network plug on the machine, it came with the board we used …”

„The system cannot be patched because we need to get the certification first…“

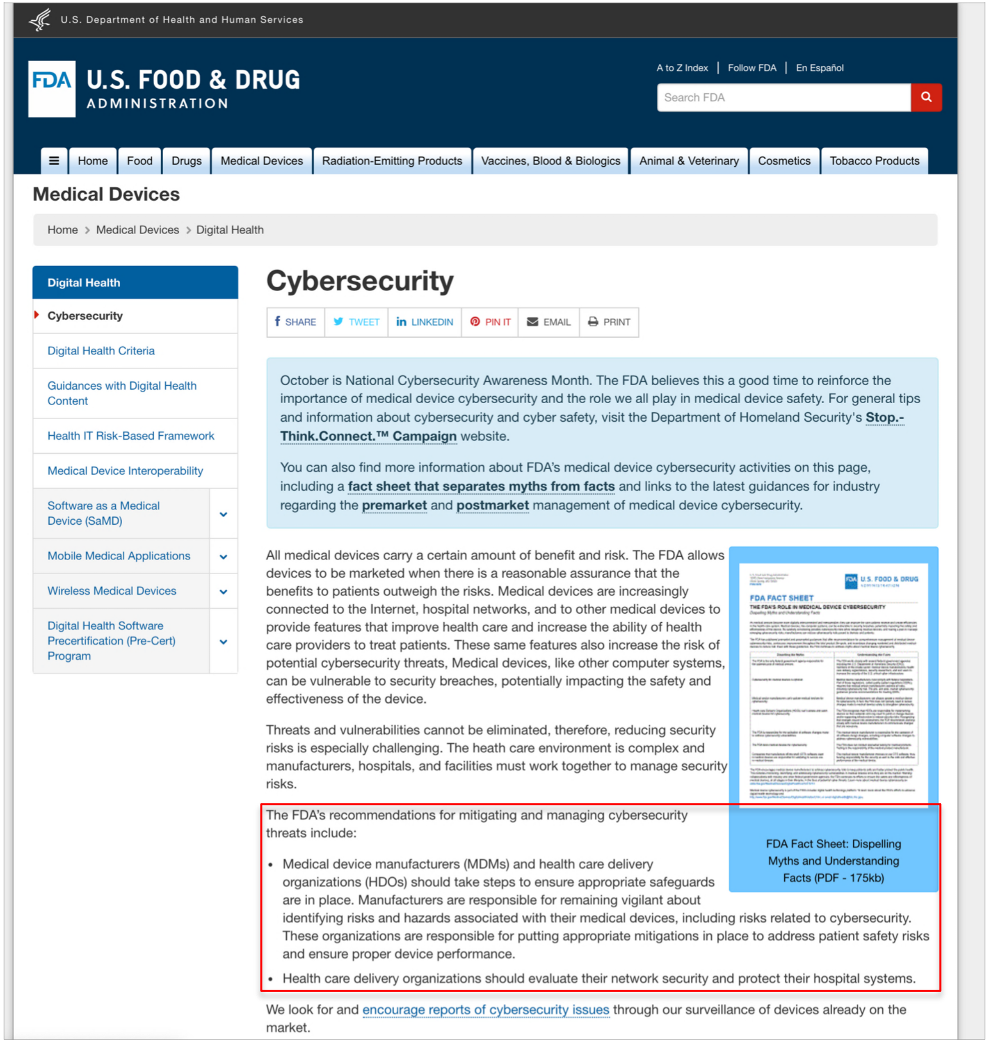
„… if we do not use encryption we can‘t do it wrong…“

„Our device will only be operated in secure environments…“

Photo by Joshua Coleman on Unsplash

Therapy

Recommendations



U.S. Department of Health and Human Services
FDA U.S. FOOD & DRUG ADMINISTRATION
A to Z Index | Follow FDA | En Español
Search FDA
Home
Food
Drugs
Medical Devices
Radiation-Emitting Products
Vaccines, Blood & Biologics
Animal & Veterinary
Cosmetics
Tobacco Products

Medical Devices

Home > Medical Devices > Digital Health

Digital Health
Cybersecurity
Digital Health Criteria
Guidances with Digital Health Content
Health IT Risk-Based Framework
Medical Device Interoperability
Software as a Medical Device (SaMD)
Mobile Medical Applications
Wireless Medical Devices
Digital Health Software Precertification (Pre-Cert) Program

Cybersecurity

SHARE
TWEET
LINKEDIN
PIN IT
EMAIL
PRINT

October is National Cybersecurity Awareness Month. The FDA believes this a good time to reinforce the importance of medical device cybersecurity and the role we all play in medical device safety. For general tips and information about cybersecurity and cyber safety, visit the Department of Homeland Security's **Stop.-Think.Connect.™ Campaign** website.

You can also find more information about FDA's medical device cybersecurity activities on this page, including a **fact sheet that separates myths from facts** and links to the latest guidances for industry regarding the **premarket** and **postmarket** management of medical device cybersecurity.

All medical devices carry a certain amount of benefit and risk. The FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks. Medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices to provide features that improve health care and increase the ability of health care providers to treat patients. These same features also increase the risk of potential cybersecurity threats, Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device.

Threats and vulnerabilities cannot be eliminated, therefore, reducing security risks is especially challenging. The heath care environment is complex and manufacturers, hospitals, and facilities must work together to manage security risks.

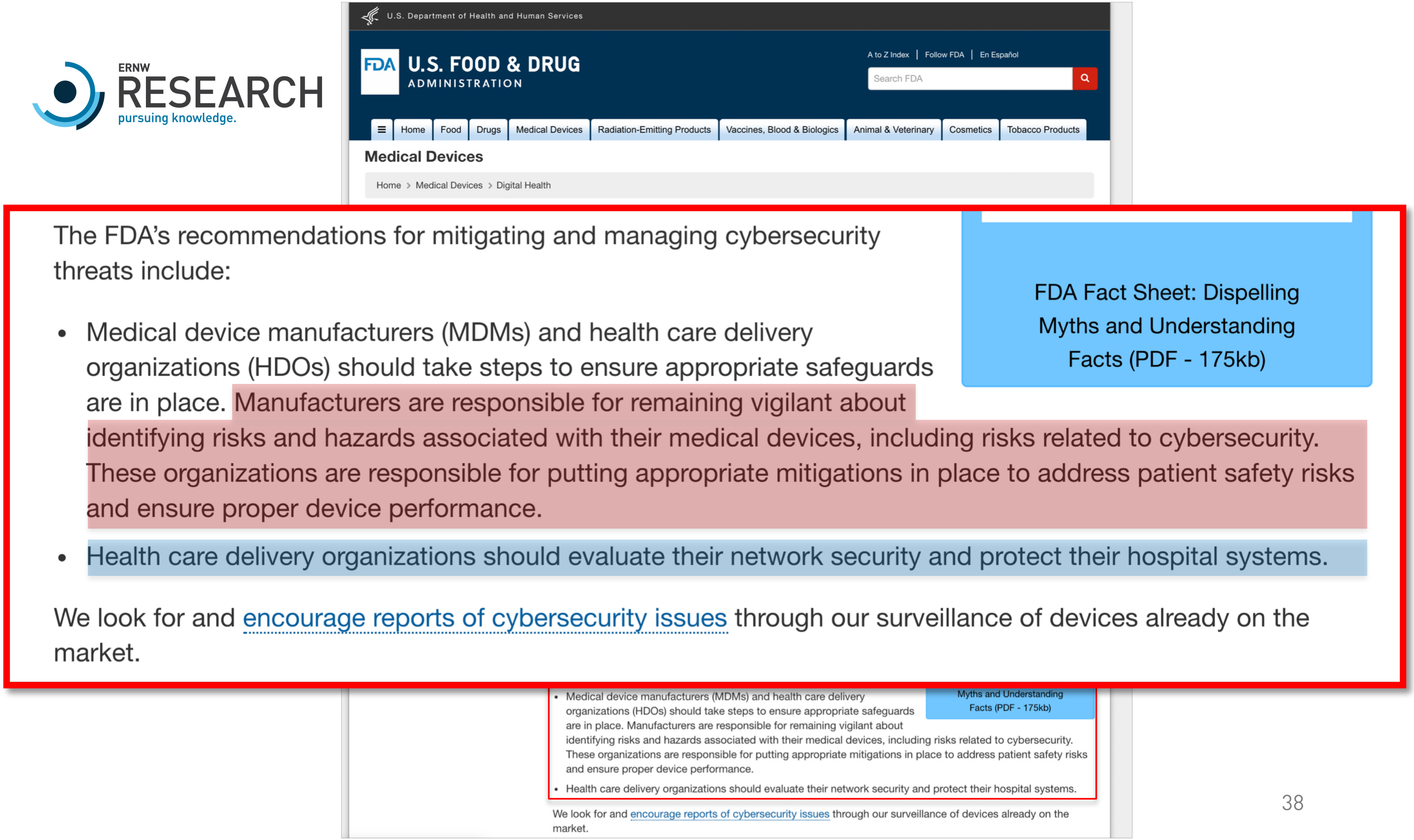
FDA Fact Sheet: Dispelling Myths and Understanding Facts (PDF - 175kb)

The FDA's recommendations for mitigating and managing cybersecurity threats include:

- Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. These organizations are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
- Health care delivery organizations should evaluate their network security and protect their hospital systems.

We look for and encourage reports of cybersecurity issues through our surveillance of devices already on the market.

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm



U.S. Department of Health and Human Services
FDA U.S. FOOD & DRUG ADMINISTRATION
A to Z Index | Follow FDA | En Español
Search FDA
Home
Food
Drugs
Medical Devices
Radiation-Emitting Products
Vaccines, Blood & Biologics
Animal & Veterinary
Cosmetics
Tobacco Products

Medical Devices

Home > Medical Devices > Digital Health

The FDA's recommendations for mitigating and managing cybersecurity threats include:

- Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. These organizations are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
- Health care delivery organizations should evaluate their network security and protect their hospital systems.

We look for and encourage reports of cybersecurity issues through our surveillance of devices already on the market.

FDA Fact Sheet: Dispelling Myths and Understanding Facts (PDF - 175kb)

- Medical device manufacturers (MDMs) and health care delivery organizations (HDOs) should take steps to ensure appropriate safeguards are in place. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. These organizations are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.
- Health care delivery organizations should evaluate their network security and protect their hospital systems.

Myths and Understanding Facts (PDF - 175kb)

We look for and encourage reports of cybersecurity issues through our surveillance of devices already on the market.

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

- Following recommendations increases the chance that the device passes FDA review
- Audience: Medical Device Manufacturers
- Differences to version from 2014:
  - Detailed documentation for design and implementation
  - Medical device security is a shared responsibility
  - Assess risks and mitigations throughout the product’s lifecycle
  - Cybersecurity Bill of Materials (CBOM)

[https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf, 2019-03-10]

FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

- Cybersecurity Bill of Materials (CBOM)
  - Listing commercial, open source, OTS software & hardware
  - Enable users (= patients, providers, HDOs) to:
    - Effectively manage their assets
    - Understand the potential impact of vulnerabilities to the device
    - Deploy measures to maintain essential device performance
- Effect: Medical Devices are <u>no black boxes</u> anymore

[https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf, 2019-03-10]

CS-132: Cyber Security Requirements for Network-Connected Medical Devices

- 2018/05: German Federal Office for Information Security (BSI)
- Best practices for manufacturers of network-connected medical devices
- Intention:
  - Accompany regulatory requirements
  - Support implementation and maintenance with focus on security
  - Assistance on how to reduce security issues from the risk analysis

[https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.html, 2019-03-10]

CS-132: Cyber Security Requirements for Network-Connected Medical Devices

- Distinction of the modes of operation:
  - Medical operation mode: Used for its intended medical purpose
  - Device configuration (incl. patient-specific parameters)
  - Technical maintenance (Updates + basic calibrations or adjustments)
- The required security measures must not have a negative impact on the safety functions of the medical devices and therefore on the lives of patients

[https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.html, 2019-03-10]

Outlook & Future Research

Challenges & Further Research

- Risk Scoring in medical environments
  - CVSS does not reflect the clinical environment + patient safety impacts
  - Approaches:
    - Rubric for Applying CVSS to Medical Devices https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices
    - Risk-Scoring System for Medical Devices (RSS-MD) https://riskscoringsystem.com/medical/
- Raising awareness in the medical community

Funded Research: Project „ManiMed“

- German Federal Office for Information Security (BSI)
- Manipulating Active Medical Devices (ManiMed)
  - Collection of recent marketed ”smart” medical devices
  - Security assessment of networked medical devices (e.g. pacemakers, insulin pumps, patient monitors, syringe pumps)
  - Publication of the security analysis and outlook for the medical care
  - Planned with a duration of 1.5 years

ERNW RESEARCH pursuing knowledge.

References

- **Julian Suleder, Dr. Andreas Dewald, Florian Grunow**; ERNW Whitepaper 66: Medical Device Security: A Survey of the Current State; Online: https://ernw.de/en/whitepapers/issue-66.html; 2018.

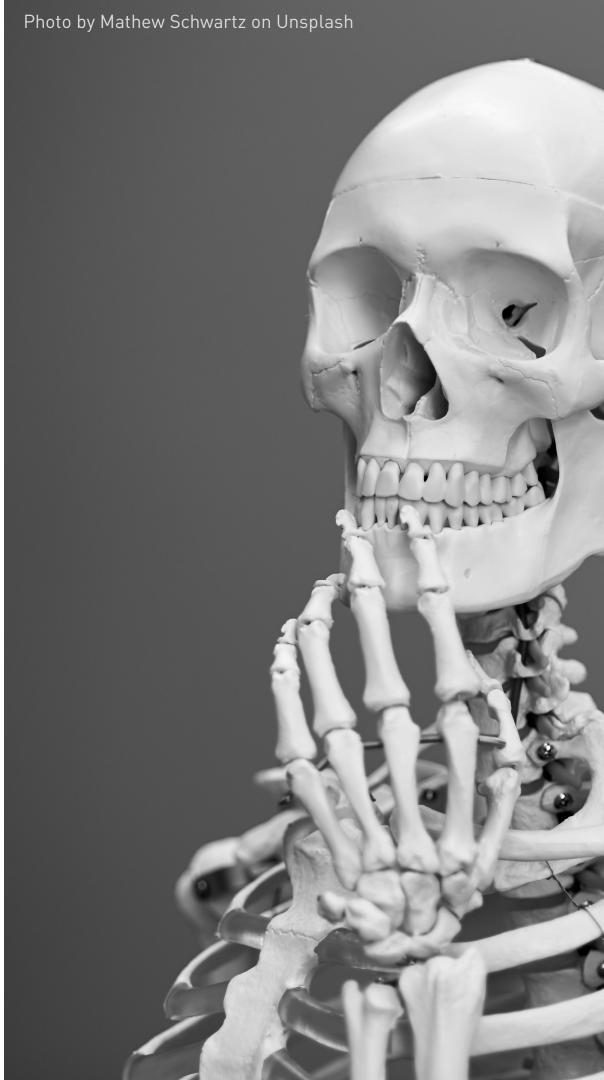


Photo by Mathew Schwartz on Unsplash

ERNW RESEARCH
pursuing knowledge.

Thank you for your Attention!

For information on risks and side-effects of this presentation please ask your doctor or pharmacist.

✉ jsuleder@ernw.de

@jsuleder

www.ernw.de

www.insinuator.net