SOFTWARE/HARDWARE VULNERABILITIES

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CC BY NC

Table of Contents

Co-funded by the European Union

FACTSHEET – SOFTWARE/HARDWARE VULNERABILITIES

1. Definition

It consists of weaknesses or flaws in software or hardware systems that can be exploited by threat actors to gain unauthorised access, disrupt services, or compromise data1. Examples include unpatched software bugs, misconfigurations, outdated operating systems, or insecure medical devices.

2. General importance

Nowadays, software/hardware vulnerabilities are a central concern. With the emergence of digital systems, almost every sector depends on interconnected software and hardware.

Abuse of these vulnerabilities could lead to significant cyber events like ransomware attacks, identity theft, or the closure of critical services2. Therefore, addressing these vulnerabilities is crucial for global cybersecurity, economic stability, and the protection of citizens' personal information.

Weak spots do not refer to isolated technical difficulties, but rather to global risks that affect multiple sectors worldwide. Thereby, managing weaknesses through systematic patching, monitoring, and coordinated disclosure is essential to making society more cyber resilient at all levels2.

3. Importance in health and care, and impact in quality of care

Healthcare is particularly vulnerable to this type of cyber threat due to its dependence on medical devices, electronic health records, and critical infrastructure that frequently operate on obsolete, challenging-to-update systems.

Software/hardware vulnerabilities are a significant underlying cause of security incidents, with 80% of healthcare organisations citing them as the source of more than 61% of their security incidents. These vulnerabilities are a constant source of concern, particularly for outdated systems and complex IT infrastructures1.

The impact of software/hardware vulnerabilities on quality of care is wide. It compromises patient safety by disrupting services, which force appointment cancellations or rescheduled surgeries. Furthermore, if attackers target medical devices such as infusion pumps, ventilators, or imaging devices, they can directly harm patients.

4. What can I do as a healthcare professional?

- Have good cyber hygiene and install updates on devices and software you use on your daily work.
- Be alert to cyber threats (phishing emails, suspicious links) and immediately report any irregularities.
- Follow your hospital protocol and make sure to respect security guidelines.
- Take part in cybersecurity training and keep up with how to respond to incidents and the impact of patient data protection.

5. More information

5.1 Learning Materials

- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Cibersecurity training from National Cryptographic Centre of Spain. Requires National login (JGT-8)
- An article on security strategies applicable to electronic patient records (IST-37)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- A compendium on the processing of patient data on online platforms. (IST-40)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context (PRAMMER-31)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)

5.2 Relevant Videos

This video discusses common software and hardware issues that can arise with medical devices and provides practical advice on how to make them safer and protect patient safety.

Cybersecurity in Healthcare | Importance of Cybersecurity in Healthcare
https://youtu.be/aZLGYxupCrQ?si=MZNID_ADom2kh8aO

The following video provides an overview of common software and hardware vulnerabilities in medical devices, as well as practical strategies for improving cybersecurity and ensuring patient safety.

Medical Device Cybersecurity | Tarlogic Security
https://youtu.be/JdOvvCP7uyE?si=KRQXpNjpoSzm0oye

5. 3 Relevant Links

This article revealed 993 flaws in medical devices and products, 160 of which could be used as weapons and 101 of which were becoming more common in the wild. It emphasizes the need for proactive cybersecurity measures in healthcare settings.

https://industrialcyber.co/medical/healthcare-research-report-reveals-exploitable-vulnerabilities-that-allow-hackers-to-breach-devices-systems/

This article discusses common security flaws in medical devices, such as data that isn't encrypted and APIs that aren't secure, and offers manufacturers advice on how to make their products safer.

https://www.vumetric.com/blog/medical-device-vulnerabilities-top-8-cybersecurity-vulnerabilities/

6. Bibliography

Souppaya, M., & Scarfone, K. (2022). Guide to enterprise patch management planning:

https://doi.org/10.6028/nist.sp.800-40r4

ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal.

https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.