White Paper

dellfer

HEALTH - ISAC NAVIGATOR™ PROGRAM

Ensuring the Safety and Security of the Medical Device Ecosystem[1]: Addressing a Major Healthcare Challenge

www.dellfer.com

Introduction

The healthcare industry faces security challenges with its healthcare information systems and medical devices. Healthcare organizations are constantly under attack, resulting in significant fiscal impact and endangering patient safety and care delivery. A recent study by Proofpoint and the Ponemon Institute[2] surveyed 641 IT and IT security practitioners in healthcare organizations. A major purpose of the survey was to determine the impact of cyber-attacks on patient safety and care delivery. The survey found 89 percent of respondents had cyber-attacks over the past 12 months. The Ponemon Institute also found that cyber-attacks cause more than twenty percent of impacted healthcare organizations to suffer increased mortality rates.[3] The most common consequences of cyber-attacks are delayed procedures and tests, resulting in poor patient outcomes for 57% of the healthcare providers and increased complications from medical procedures for half of them.[4] In addition, Ponemon reported survey responders believed that insecure medical devices were the cybersecurity threat of greatest concern.

The Food and Drug Administration (FDA) is aware of the impacts of cyber-attacks and has recently issued draft guidance[5] for medical devices. In the report, the FDA states:

> “…cybersecurity threats to the healthcare sector have become more frequent and more severe, carrying increased potential for clinical impact. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the U.S. and globally. Such cyber-attacks and exploits may lead to patient harm as a result of clinical hazards, such as delay in diagnoses and/or treatment…. increased connectivity has resulted in individual devices operating as single elements of larger medical device systems. These systems can include health care facility networks, other devices, and software update servers, among other interconnected components. Consequently, without adequate cybersecurity considerations across all aspects of these systems, a cybersecurity threat can compromise the safety and/or effectiveness of a device by compromising the functionality of any asset in the system. As a result, ensuring device safety and effectiveness includes adequate device cybersecurity, as well as its security as part of the larger system.”[6]

Additional cybersecurity steps beyond current measures must be taken. The highest return on an incremental investment is improved cybersecurity for medical devices. There are two reasons for this. First, the Ponemon survey found that medical devices represent the greatest cyber threat. Second, the FDA already regulates medical devices and is developing new lifecycle cybersecurity regulations for them. This is illustrated in the draft FDA guidance that states:

> “…the rapidly evolving landscape, an increased understanding of emerging threats, and the need for capable deployment of mitigations throughout the total product lifecycle (TPLC) warrants an updated, iterative approach to device cybersecurity.”[7]

Clearly, it is logical to focus on cybersecurity improvements in medical device security and safety. In the following section, we will address the steps the healthcare industry should take to ensure that the medical device software is developed using best practices and associated standards for security and safety. In the last section, the paper will propose a solution for implementing the best cybersecurity and safety protection for the medical device during operation.

Software Development and the Software Supply Chain

Today, most companies develop software using a combination of self-developed code, vendor code, and free and open-source software. The Linux Foundation estimates that free and open-source software (FOSS) constitutes 70-90% of any given piece of modern software[8]. Given the potential vulnerabilities of such a combination of software, organizations must keep a comprehensive and ongoing cybersecurity supply chain risk management program as part of their software development process. Therefore, during the software acquisition, healthcare organizations should ensure vendors have a rigorous software supply chain process like the one discussed in the next section.

The need for of a well-managed software supply chain program is demonstrated by the SolarWinds Sunburst cybersecurity attack by Russian hackers who successfully compromised many of the largest technology companies, the US government, and a hospital chain.[9] The source of the attack was the compromised SolarWinds Orion Platform, an infrastructure monitoring and management platform for IT administration[10]. For details of how the attack was successful and suggestions for mitigation, see https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth.

Great skill, time, and resources were used to inject malware that would not be detected in code reviews or by cybersecurity tools. The attacker’s key first step was the compromise of a single Microsoft email account,[11] which provided entry into the SolarWinds network and eventual access to the SolarWinds software development process. This led to the compromised software product being installed on thousands of networks and having trusted, privileged network access. Once deployed in these networks, the cyber-attackers could open a backdoor into thousands of networks.

The SolarWinds Sunburst attack is just one of many successful compromises attackers achieve. According to a study by Argon Security, an Israeli cybersecurity firm specializing in protecting the integrity of the software supply chain, these attacks grew by more than 300 percent in 2021 compared to 2020. Another recent study of more than 400 IT executives and managers by Anchore Enterprise, a California-based developer of a security-centric software supply chain management platform, found that three in five companies in 2021 were targeted by software supply chain attacks[12].

Vendor products, especially security tools with privileged access or control over computer networks, become high-priority targets for threat actors. This is because a compromise of these tools provides attackers authorization to network resources, data, and applications. So, from a security perspective, all software in an ecosystem should have the same rigor for security during its development. A simple definition of an ecosystem in this paper is a grouping of applications and hardware that directly interact with each other.

Software Development Process Protections at the Supply Chain Level

This paper will discuss steps to ensure that your medical device ecosystem software supply chain meets the level of security necessary for the healthcare industry. A good starting point is a recently published document by the National Institute of Standards and Technology (NIST) entitled “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.” This publication supplies guidance to organizations on how to find, assess, and mitigate cybersecurity risks throughout the supply chain at all levels of their organizations.[13]

According to the (NIST) software supply chain report, common attack techniques against an organization’s software development process are hijacking updates, undermining code signing, and compromising open-source code.[14] As part of a cybersecurity supply chain risk management program for medical devices, verify that all medical device vendor software and software used in the medical device ecosystem use a software development lifecycle process that:

- Implements mitigations against common software development attacks per NIST report.
- Is compliant with International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 62304 standard.
- Looks for known weaknesses in their source code and compiled code.
- Highlights and verifies all new code against new requirements for each new build.
- Ensures that the software development process is segmented from the rest of the organization’s computer infrastructure, monitored for security issues, and subjected to routine penetration testing.

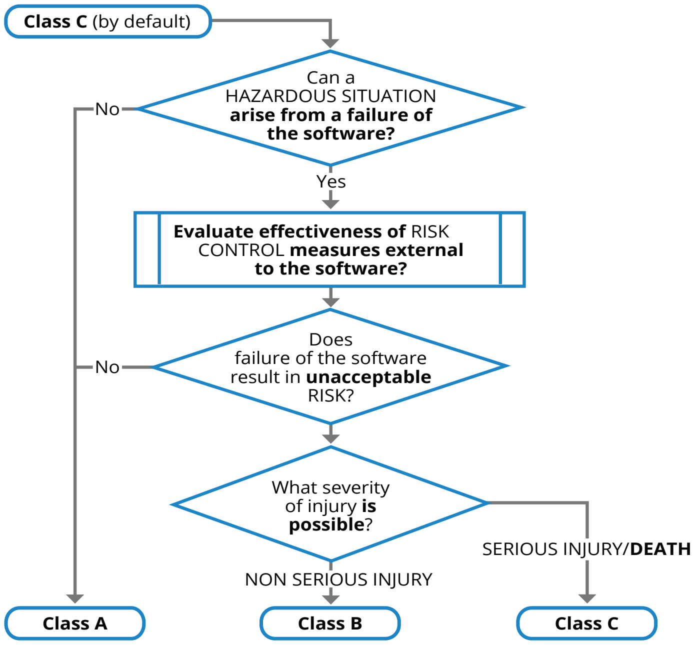
- Actively finds and discloses vulnerabilities and maintains a vulnerability response program.
- Supplies a software bill of material (SBOM) that supplies details of all the software components. The SBOM community has developed three existing data standards (formats) that can convey the data fields and should be used to support the automated, machine-readable transfer of information. These formats are SPDX, CycloneDX, and SWID tags[15]. If a vendor cannot supply a SBOM, consider using that as a differentiator when selecting among competing products.
- Verifies that their vendors' supply chain risk process addresses any issues, including vulnerabilities and potential malware in open-source software included in their vendors' products[16].

What Is ISO/IEC 62304

The international standard IEC 62304 ("MEDICAL DEVICE software – Software lifecycle processes") provides requirements for developing and maintaining medical device software. Initially published in 2006, it was amended in 2015 to apply a risk-based approach to the safety classification of medical device software and to provide clarity on how to deal with legacy software. Following IEC 62304 enhances the reliability of a device's software by requiring diligence in design, testing, and verification, ultimately improving the overall safety of the medical device. For medical devices, IEC 62304 specifies three safety classes and the level of rigor in the software development process for each class. These classes are:

- **Class A:** No injury or damage to health possible
- **Class B:** Injury possible, but not serious
- **Class C:** Death or severe injury possible

The higher the safety risk there is a corresponding increase in the rigor needed for the software development process.[17] The class of a device is decided by the severity of the consequences of a failure in the device software. This chart below illustrates the IEC schematic below, which is used to determine device classification.


Class C (by default)
Can a HAZARDOUS SITUATION arise from a failure of the software?
No
Yes
Evaluate effectiveness of RISK CONTROL measures external to the software?
Does failure of the software result in unacceptable RISK?
No
What severity of injury is possible?
SERIOUS INJURY/DEATH
NON SERIOUS INJURY
Class A
Class B
Class C

In determining the software safety classification of the SOFTWARE SYSTEM:

- **Probability of a software failure shall be assumed to be 1.**
- **Only** RISK CONTROL **measures not implemented within (external to) the** SOFTWARE SYSTEM **shall be considered.**

NOTE: **Such** RISK CONTROL **measures may reduce the probability that a software failure will cause HARM, and/or the severity of that HARM.**

NOTE: **A** SOFTWARE SYSTEM **which implements** RISK CONTROL **measure may fail, and this may contribute to a** HAZARDOUS SITUATION**. The resulting** HARM **may include the** HARM which the RISK CONTROL **measure is designed to prevent.**

IEC

Source: Medical device software — Software life cycle processes: IEC 62304:2006+AMD1:2015

IEC 62304 is a widely adopted standard in Europe and the United States. It covers firmware in medical device hardware devices and software acting as a medical device. The FDA recognizes IEC 62304 as a consensus standard.[18] A new draft (2021) IEC 62304 version extends the scope beyond medical devices to all health software.[19]

Since IEC 62304 has been harmonized with the Medical Device Directive in the EU and is recognized as a Consensus Standard by the FDA in the US, it can be used as a benchmark to follow regulatory requirements in both markets. To date, this standard has been recognized in most countries that use compliance standards to fulfill regulatory requirements.

Operational Ecosystem of Medical Devices

The FDA expects that cybersecurity for medical devices be addressed during the development process as well as during the operational deployment and use of the medical device. Given the FDA and healthcare security staff's concerns regarding medical devices, it is sensible to take additional steps to protect the medical device operational environment. For security and safety reasons, medical devices and their ecosystem should be segmented from other parts of the healthcare system. Any software product deployed within the medical device segment is part of the medical device ecosystem.

The marketplace offers multiple products to provide that segmentation. It is recommended that all software within the ecosystem should be developed using the same safety and security standards that were used for medical device development. Developers of software intended to be within a medical device ecosystem should follow IEC 62304 to determine the rigor of the software development process.

For Class C (death or serious injury) medical devices, all the ecosystem software should be developed to IEC 62304 Class C requirements. Class B (injury possible) and Class A (no injury possible) require less rigorous IEC 62304 development standards. In all cases, the practices recommended by NIST and the additional steps mentioned in the Software Development Process Protections section should be followed.

Manufacturers should conform to standards with the justification that cyber attackers will look for the weakest link to target. For example, if a vendor's software was compromised during the software development process, attackers could use it to compromise other software within its ecosystem. Added security measures such as a data diode[20] can be utilized to limit incoming traffic to the medical device from outside its segment. The data diode would not block outgoing traffic from the medical device.

In the near term, changing all the medical device ecosystem applications to the same development standards is not feasible. However, it should be a goal of the healthcare technology industry. The initial focus should be on IEC 62304 Class C medical devices where a malfunction could cause death or serious injury. Any system that is required to support the Class C medical device but does not comply with the security and safety requirements should be isolated using different technologies to ensure only appropriate data is exchanged between that system and the medical device.

The providers of systems that support medical devices need to recognize the marketplace's need for more rigorous security and safety requirements. It is critical that device manufacturers tailor their products to the healthcare industry 's operational requirements, and safety and security standards.

References

1. In this paper it is assumed for security and safety reasons the medical devices will be segmented from the rest of the healthcare systems and the ecosystem are the application and hardware that are included in the medical device segment
2. Proofpoint and the Ponemon Institute, "Cybersecurity Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care, September 8, 2022
3. Globalnewswire September 8, 2022, "New Ponemon Institute Study Finds that Cyberattacks Cause More than Twenty Percent of Impacted Healthcare Organizations to Experience Increased Mortality Rates
4. Globalnewswire September 8, 2022, "New Ponemon Institute Study Finds that Cyberattacks Cause More than Twenty Percent of Impacted Healthcare Organizations to Experience Increased Mortality Rates
5. FDA "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Draft Guidance for Industry and Food and Drug Administration Staff" April 8, 2022
6. FDA "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Draft Guidance for Industry and Food and Drug Administration Staff" April 8, 2022
7. FDA "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Draft Guidance for Industry and Food and Drug Administration Staff" April 8, 2022
8. https://www.linuxfoundation.org/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on/#:~:text=Introduction,and%20non%2Dtech%20companies%20alike
9. https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402
10. www.solarwinds.com
11. https://www.techtarget.com/searchsecurity/news/252495885/SolarWinds-Office-365-environment-compromised
12. https://securitytoday.com/articles/2022/05/31/software-supply-chain-attacks-are-skyrocketing.aspx
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
14. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
15. https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations
16. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

17. https://medium.com/retina-ai-health-inc/iec-62304-medical-device-software-lifecycle-processes-2b7967577c3f

18. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfstandards/detail.cfm?standard__identification_no=38829

19. https://blog.cm-dm.com/post/2021/02/19/IEC-62304%3A2021-Committee-Draft-Version%3A-Groundhog-Day

20. In electronics a diode is a component that allows current to flow in one direction only. Similarly, this concept has been applied to data communications. Data diode technology lets information flow in only one direction, from secure areas to less secure systems, without allowing reverse access