TAG CYBER

PROTECTING MEDICAL DEVICES FROM CYBER EXPLOITATION

DAVID NEUMAN, SENIOR ANALYST, TAG CYBER

TAG CYBER

PROTECTING MEDICAL DEVICES FROM CYBER EXPLOITATION

DAVID NEUMAN, SENIOR ANALYST, TAG CYBER

This article explains the urgency and unique challenges of protecting medical devices from cyberattacks and exploitation.

INTRODUCTION

The urgency is building. With the passage of December's Omnibus Bill, policymakers have signaled that it's time to get serious about medical device cybersecurity.

The Omnibus Bill, which incorporates parts of the Patch Act, gives the Food and Drug Administration (FDA) statutory authority to regulate medical device cybersecurity. The FDA has long contemplated taking a stronger stance to regulate the cybersecurity of medical devices, as evidenced by documents published by the agency regarding the pre-market submission process as well as the post-market management of medical device cybersecurity.

The Omnibus Bill grants the FDA statutory authority as of March 29, and it signals that software bill of materials (SBOMs) will be a key part of prioritizing medical device cybersecurity when the FDA begins reviewing new submissions for cybersecurity requirements. Devices will be designed from a secure development perspective, and there will be post-market management processes that monitor and respond to new and emerging vulnerabilities.

Indeed, the Omnibus Bill signals a shift in regulatory perspective on the issue of medical device cybersecurity. With its passage, the government and the agencies it charges with enforcing medical device safety have said that transparency in cybersecurity is now intrinsically tied to a device's quality. In others words, if your device can be manipulated to function in an unexpected manner, that's now a quality issue.

The importance of protecting medical devices from cyberattacks isn't to protect the device itself, the data or the networks where they reside. ***It's to protect and preserve the well-being and safety of human life,*** a key component of the FDA's role in the United States as it seeks to regulate the country's medical devices.

MEDICAL DEVICE CYBER RISKS

Despite, and owing to the importance of, current and emerging regulatory requirements, in 2022, Cyber Security Works (CSW) researchers identified 624 vulnerabilities that attackers could exploit to target a healthcare facility. Of these, 43 were weaponized and 12 were trending in the wild. Advanced persistent threat groups were exploiting four, and two were associated with ransomware. In addition, CSW investigated 56 vendors and 846 products and found the highest number of vulnerabilities (64%) in software applications used in the healthcare industry.

WHAT MAKES MEDICAL DEVICES UNIQUE?

In some respects, medical devices are like industrial control systems because they perform specialized functions and, in many cases, use proprietary software to perform those functions. Compared to computer and network systems designed to be managed and sustained as part of the enterprise, medical device software cannot gain visibility and automate to act quickly to remediate dangerous weaknesses or flaws.

Providing lifesaving care to people in healthcare facilities depends on technology for many services, such as imagery, monitoring vital signs and administering medications. These are each unique technology systems with their own manufacturing and software supply chains. Combine this with open-source code and a fragmented view of past, current and emerging vulnerabilities, and you have a high-risk environment that could jeopardize human life.

MEDICAL DEVICES ARE MOST SUSCEPTIBLE TO TWO TYPES OF THREAT VECTORS:

- **Device-based threats** include firmware and software vulnerabilities, which attackers can exploit to gain unauthorized access to medical devices and the data they collect.
- **Supply chain threats** include threats to the integrity and authenticity of software and firmware updates delivered to medical devices.

A HOLISTIC APPROACH TO MEDICAL DEVICE SECURITY AND RESILIENCE

A report by Statista estimated that there were around 26 billion interconnected devices worldwide in 2019. This number is expected to reach 75 billion by 2025. Related to this, a report by Grand View Research published in 2020 indicated that the global internet of medical things (IoMT) market is expected to reach $254.2 billion by 2026, growing at a CAGR of 23.4% from 2019 to 2026. The report predicts that connected medical devices will increase significantly during this period.

The types of products in this growth include fetal monitoring devices, ventilators, anesthesia machines, and imaging systems. Their numbers will grow not only in hospitals and clinics, but also in nursing homes, assisted living facilities, long-term care centers and home care settings. Organizations responsible for the security of medical devices must have the following capabilities in an efficient platform to maintain a robust security posture and act quickly.

- **Deep insight.** Access to critical information about product components and security issues inherited from vendors and third-party components, including known vulnerabilities, common weaknesses and insecure configurations.
- **Automate to scale. Reduce or eliminate manual testing.** Perform testing processes throughout the development lifecycle across product portfolios and business units.
- **Act decisively.** Prioritize based on risk criticality and remediate by ensuring corrective actions are taken and implemented effectively.

Understanding these ecosystems' software supply chains is critical to a holistic approach to software security. The software supply chain is essential to the IoMT ecosystem as it's how manufacturers deliver devices, applications and systems. However, this supply chain is not immune to cybersecurity risks, such as inserting malicious code or exploiting vulnerabilities. These risks are now more significant as IoMT devices become more prevalent and interconnected.

IoMT cyber practitioners must understand the risks in their software supply chains and know how and when to mitigate them. In addition, they must ensure the supply chain is secure and meets standards while enabling continuous visibility. Here are some of the steps that cyber practitioners should take to achieve this:

• Identify and assess risks: The first step is identifying and assessing the potential risks in the software supply chain by evaluating software suppliers, third-party vendors and other stakeholders to determine their security posture, vulnerabilities and possible threats. They should also evaluate the software development process and assess the security controls.

- **Establish security standards:** Establish security standards and policies that all stakeholders in the software supply chain must follow. These standards should cover secure coding practices, vulnerability management, testing and incident response.
- **Implement security controls:** Implement security controls that prevent or detect software supply chain attacks. These controls may include secure communication protocols, digital signatures, code reviews and access controls.
- **Monitor the supply chain:** Continuously monitor the software supply chain to detect any potential risks or anomalies. They should have visibility into all aspects of the supply chain, including the software development process, deployment and maintenance.
- **Conduct regular assessments:** Regularly assess the software supply chain to ensure it remains secure and meets standards. These assessments should cover all stakeholders and processes involved in the supply chain.
- **Develop a response plan:** Develop a response plan outlining the steps to take in a software supply chain attack. The plan should include incident response procedures, communication protocols and recovery strategies.

AUTOMATE SBOMS THROUGH THE DEVICE DEVELOPMENT LIFECYCLE

Because of the diversity and complexity of the software supply chain, the SBOM is essential for several reasons. An SBOM promotes transparency in the supply chain by providing information about the origin, version and licensing of the software components used in the product. This information is critical to identify potential security vulnerabilities, assess risks and make informed product development and maintenance decisions. It also helps manufacturers identify and manage risks associated with using third-party software components in their products. Manufacturers can mitigate potential risks and protect products by knowing which software components are used and understanding their security and quality attributes.

Establishing these insights can be highly time-consuming, so let's look at how medical device manufacturers can automate SBOMs through the entire device development lifecycle by implementing the following steps:

- **Implement an automated software composition analysis (SCA) tool:** An SCA tool can automatically analyze the software components used in the development process and generate a comprehensive SBOM. In addition, this tool can scan the software codebase and identify all the open-source and third-party components used in the project.
- **Establish a central repository for SBOMs:** Medical device manufacturers can create a centralized repository to store all SBOMs generated throughout the development process. This repository can be used as a single source of truth for all stakeholders involved in the project.
- **Automate the SBOM generation process:** Automate the SBOM generation process by integrating the SCA tool with the development process. This ensures that each software release generates the SBOM automatically and accurately.
- **Integrate SBOMs with the supply chain:** Integrating SBOMs with the supply chain allows manufacturers to track the software components used in the device and identify any potential vulnerabilities. This can help manufacturers address issues before they become a problem.
- **Ensure SBOMs are up to date:** As the device development process evolves, new software components may be added, modified or removed. Therefore, ensuring that the SBOM is kept up-to-date throughout the device development lifecycle is crucial.

By implementing these steps, medical device manufacturers can automate the SBOM generation process and streamline the device development lifecycle. This can help manufacturers ensure compliance with industry regulations and enhance the security and safety of their devices.

CONCLUSION

Digital transformation has brought about a revolution in the way products are built, distributed and connected. With the advent of new technologies such as IoMT, artificial intelligence and big data analytics, businesses can achieve greater efficiencies, productivity gains and increased profitability.

However, this transformation has also increased the number of network-connected devices, users and apps, leading to an expanded attack surface that has attracted bad actors looking for ways to exploit vulnerabilities in these systems. While device manufacturers must meet a set of criteria to ensure the security of their products, this does not guarantee continuous protection against exploited vulnerabilities.

One of the main reasons device manufacturers cannot ensure continuous protection is the dynamic nature of security threats. Bad actors constantly evolve their attack methods, and new vulnerabilities are discovered regularly, which makes it difficult for device manufacturers to stay ahead and address these threats promptly and effectively.

Regulatory requirements like those fostered in the Omnibus Bill will guide many device manufacturers on where to focus and how to stay on the right side of compliance, however focusing primarily on compliance with regulatory requirements can lead to a false sense of security. While compliance with these standards is essential, it only sometimes translates into continuous protection against vulnerabilities.

To address this issue, device manufacturers must adopt a proactive security approach. They must continuously monitor their products and systems for vulnerabilities and implement appropriate measures to address them as they arise. This approach requires a shift in mindset from one that views security as a one-time activity to one that recognizes it as a continuous process.

Another essential component of continuous protection is collaboration. Device manufacturers must work closely with other stakeholders in the supply chain, including suppliers, distributors and customers, to ensure that security risks are identified and addressed across the entire product lifecycle. This requires an open and transparent approach to communication and a shared commitment to security.

As medical devices and technology become more sophisticated, security teams and software developers must unify their efforts to ensure human safety. Platforms like Finite State provide the technology, processes and scalability to address today's challenges and tomorrow's emerging threats.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.