Protecting Medical Devices from Cyber Exploitation

FINITE STATE

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 heavier hand toward regulating the cyber security of medical devices as evidenced by previous documents published by the agency regarding the premarket submission process as well as the post-market management of medical device cyber security.

With the Omnibus Bill, the FDA is granted statutory authority, as of March 29, and, what's more, the bill signals that SBOMs will be a key part of making medical device cybersecurity front and center 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.

FINITE STATE

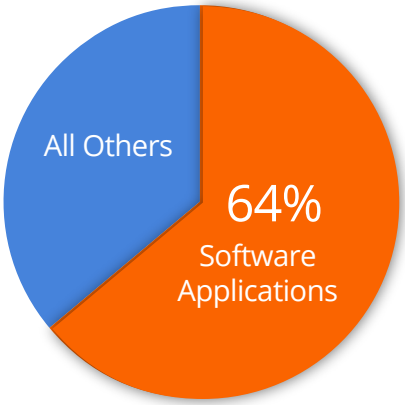
The importance of protecting medical devices from cyberattacks isn't to protect the device itself, the data, or the networks where they reside. Instead, **it's to protect and preserve the well-being and safety of human life**, a key component of the FDA's role in the United States as it seeks to regulate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

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 come out and said that transparency in cybersecurity is now an issue intrinsically tied to a device's quality. In other words, if your device can be manipulated so that it allows it to function in an unexpected manner, that's now a quality issue.

Medical devices — rising 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.

HEALTHCARE FACILITY VULNERABILITIES



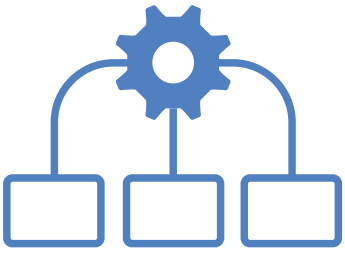
What is unique to medical devices?

In some respects, medical devices are like Industrial Control Systems (ICS) because they perform specialized functions and, in many cases, use proprietary software to perform those functions. Compared to computer and network systems in an ecosystem 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 imagery, monitoring vital signs, and administering medications, to name a few. These are all 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
including firmware and software vulnerabilities, which attackers can exploit to gain unauthorized access to medical devices and the data they collect

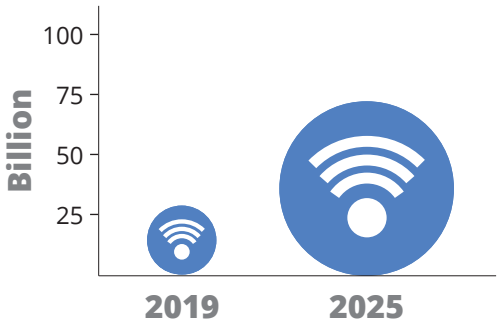


Supply ChainThreats
threats to the integrity and authenticity of software and firmware updates delivered to medical devices

A holistic approach to the security and resiliency of medical devices is needed.

In a report by Statista, it is 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.

INTERCONNECTED DEVICES WORLDWIDE



The types of products in this growth include fetal monitoring devices, ventilators, anesthesia machines, and imaging systems, to name a few. 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.

AUTOMATE TO SCALE

Reduce or eliminate manual testing. Perform testing processes throughout the development lifecycle across product portfolios and business units.

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.

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 toward software security. The software supply chain is essential to the IoMT ecosystem. It is how manufacturers deliver to devices, applications, and systems. However, this supply chain is not immune to cybersecurity risks, such as inserting malicious code or exploiting vulnerabilities. This risk has become more significant as IoMT devices become more prevalent and interconnected.

IoMT cyber practitioners must understand the risk in their software supply chains and know how and when to mitigate it. 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. Evaluate the 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.

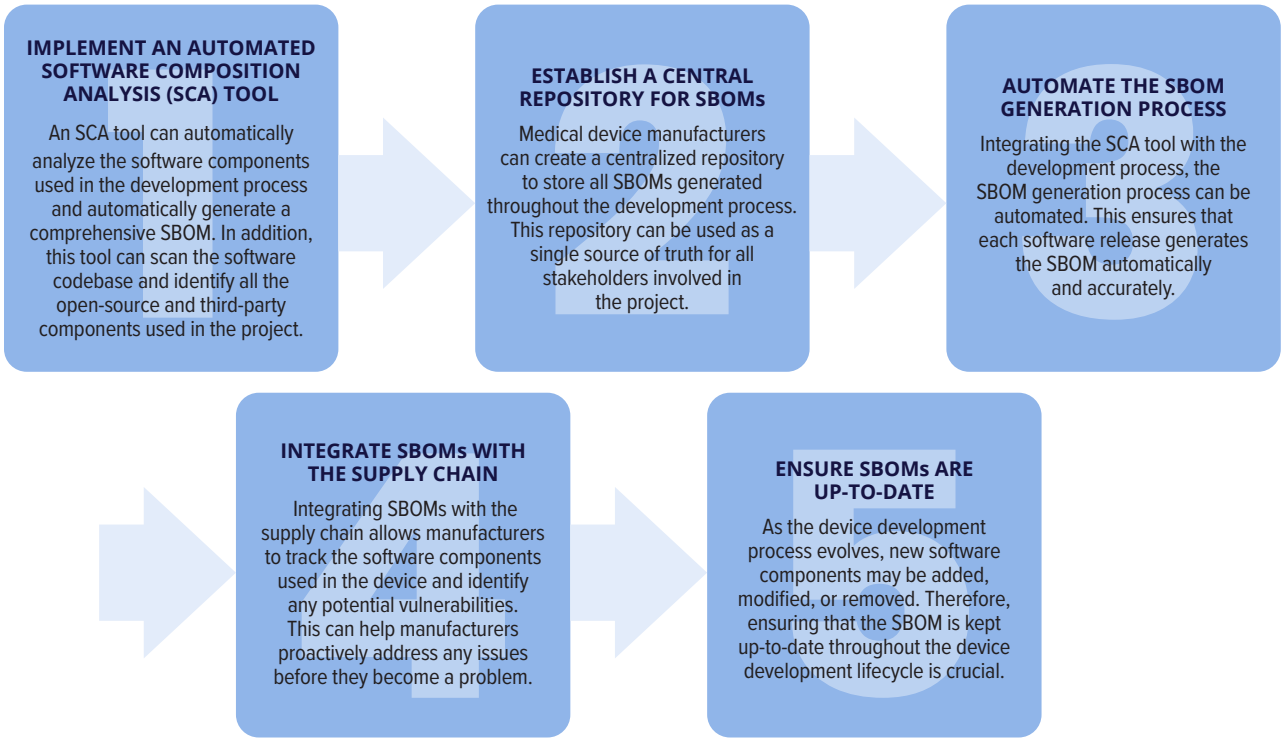
Develop a response plan: Develop a response plan outlining the steps to take in a software supply chain attack. The plan should include incident response procedures, communication protocols, and recovery strategies.

How can medical device manufacturers automate SBOMs through the entire 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 for identifying potential security vulnerabilities, assessing risks, and making 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 proactively 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 the following steps can help medical device manufacturers automate SBOMs through the entire device development lifecycle.

AUTOMATING SBOMS THROUGH THE ENTIRE DEVICE DEVELOPMENT LIFECYCLE



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 the IoMT, Artificial Intelligence (AI), 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. This expansion, in turn, has attracted the attention of bad actors continuously 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.

Regulatory requirements like those fostered by the passage of the Omnibus Bill provide guidance to 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 effort 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 Finite State

Finite State empowers organizations to gain control of application and product security for their connected devices and software supply chains. Across the software supply chain lifecycle, Finite State is the single pane of glass for customers that provides continuous visibility into software supply chain risk.

Backed by a team of seasoned experts, Finite State's platform arms customers with the automation to scale risk mitigation and 2B+ data points to deliver actionable SBOM's and insights, critical vulnerability data and the remediation guidance necessary to mitigate AppSec and product risk to protect the connected attack surface.

FINITE STATE

finitestate.io