Vulnerability Management for Medical Devices

A risk mitigation approach for health technology managers

ASIMILY

ASIMILY.COM

Vulnerability Management for Medical Devices

A risk mitigation approach for health technology managers

ASIMILY

If you are involved in technology, you know the drill: Microsoft Patch Tuesday, or Cybersecurity and Infrastructure Security Agency (CISA) releases an urgent advisory, or an Information Sharing and Analysis Center (ISAC) issues a bulletin of an urgent cybersecurity advisory to its membership.

And you have to fix them…

Yet, with many, especially complex vulnerabilities like Urgent/11, SweynTooth, or GRUB2, you don't get enough information on the actual risk impact to the organization, which devices are affected, what are the actual impacts, what is the criticality? With medical devices each of these factors are critical points that can impact patient safety and clinical operations, and you cannot simply apply the patch due to regulatory constraints on the medical device manufacturers' and their products.

In most health delivery organizations (HDOs), these cybersecurity alerts trigger change management processes and organization-wide actions to identify and patch various networked endpoints and servers to minimize network exposure and data risks from this latest vulnerability. As vulnerabilities and threats are rapidly accelerating, so are the organization's exposure and risks. With little influence to change these dynamics, the challenges are what tools and processes are in place to identify and prioritize where to focus limited resources to mitigate vulnerabilities, with patching when possible, or other mitigating control measures.

The complexities of connected devices, the variety of devices with legacy Operating systems, regulatory constraints, and alignment with clinical priorities does not always permit the rapid deployment of cyber-related patches; despite the FDA post-market guidance conveying some flexibility to meeting the threats. While some suggest this guidance from the FDA permits patching, the medical device manufacturer (MDM) ultimately remains responsible "about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity". The manufacturer is still required to conduct a risk assessment for any changes to their product and installed software to ensure the intended use of the device, and that any software changes do not alter the intended use and operation of the device. This is where the response and delay are often the reality facing HTM and CE departments.

HDOs may consider the risk of not-patching is higher than the risk of patching; in this scenario the HDO then accepts not just the risk of patching, but also the risk of unintended consequences relating to the software patch and the device(s) in use supporting patient care. This is not a stance most HDOs are comfortable taking, if they even have the capability or program maturity to lead to such a decision. Beyond the device as an end point, the FDA post-market guidance makes it clear that HDOs "should evaluate their network security and protect their hospital systems." The individual HDO has clear responsibility to maintain the secure baseline of the connected devices they purchase and put on their network. Challenge is there are a tens of thousands of vulnerabilities across thousands of devices and limited resources.

In the dynamic space of exponentially escalating cyber-threats it is essential then for an organization to determine the most critical vulnerabilities to focus their resources and efforts and to understand how to mitigate risks when no manufacturer certified patch exists or where broad network based segmentation and quarantining techniques are not easily applied or are effective (due to the challenge of applying them accurately on the network OR the risk of overloading your network appliances OR since risks of specific vulnerabilities might not get automatically mitigated by broad segmentation techniques). These capabilities are essential for the healthcare system to reduce risk, prioritize resources, and ensure patient safety and quality patient care.

Being able to prioritize across different vulnerabilities and devices across an HDO requires understanding of the individual endpoints and other factors in the environment. Not all risks are created equal and a partner that can differentiate where the main risks and priorities are can provide a great opportunity to start, and align, a connected medical device security program with the IT program. Utilizing a risk-based approach to vulnerability management along with workarounds permits the deployment and use of scarce resources on tasks that mitigate and reduce risk to the organization.

ASIMILY and the ASIMILY INSIGHT platform provides both.

Utilizing deep packet parsing, Artificial Intelligence and Machine Learning-enabled exploit analysis algorithms, ASIMILY INSIGHT's risk-based methodologies developed specifically for medical and connected devices, enables the Asimily INSIGHT platform to differentiate risk across the ANSI/AAMI/IEC 80001 risk management framework:

1. Patient Safety
2. Clinical Effectiveness
3. Data/Network Security
4. Business/Operations Impact

In addition information from Manufacturer security capabilities (MDS2s) are incorporated into the analysis to understand the high likelihood and high impact vulnerabilities and devices in the environments. Often, the identified vulnerabilities can include a mitigation recommendation so identified risks can be mitigated with other technical or administrative controls when patching is not possible. This permits a structured and strategic to the organization's connected medical device risk management program. With this capability and approach the organization can focus their limited resources (time, money, people) on risks with highest impact to the organization

In summary, patching or broad segmentation alone is not a reasonable approach to address cybersecurity and vulnerability management for connected medical devices; it is not practical and, in many cases, not possible. *ASIMILY INSIGHT* can allow our health System to save time and resources focusing on the most critical vulnerabilities and devices, mitigate risks for such devices through Asimily recommended actions and extend life for all other devices providing a Health System a true Return on Investment through Vulnerability Management.

Keep Your Medical Devices Safe From Cyber Attacks

99%
Device Accuracy on Classification

85%
Reduction in manpower

1,000
Sites deployed

FEATURES INCLUDE

INVENTORY

Monitor and Classify devices passively using machine learning, deep packet inspection and parsing; characterize security posture.

RISK MONITORING

Monitor Threats, Anomalies and Cyber-policies.

PRIORITIZE

ASIMILY prioritizes vulnerabilities with the highest likelihood and highest impact on clinical safety, business operations, and data security.

FIX

Plan mitigation of vulnerabilities using ASIMILY recommendations and block / quarantine devices if anomalies or security concerns are detected.

REPORT

Generate reports on Medical and IoT device attribute, configurable reporting tool to create reports, access any out of the box ASIMILY reports.

ASIMILY

REQUEST A DEMO TODAY

asimily.com | info@asimily.com
Tel: 1-833-274-6459 (1-833-ASIMILY)