2022 SECURITY FOR MEDICAL DEVICES

MAT CAUGHRON CISSP CSSLP NSA-IAM NSA-IEM

Where we are now…

lack of investment is catching up with healthcare device industries

hospital budget dynamics

M&A starting to drive investment $$

Here to Help:

us-cert.cisa.gov/ics

www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

www.fda.gov/medical-devices/digital-health-center-excellence/wireless-medical-devices

www.fcc.gov/document/fcc-proposes-ban-devices-deemed-threat-national-security

www.regulations.gov/docket/FDA-2021-D-1158/document

FDA Focuses on Quality

Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.

The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.

The FDA does not conduct premarket testing for medical products.
Testing is the responsibility of the medical product manufacturer.

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

FDA Contribution - Encourage Transparency and Documentation with SBOM's

Current state: emphasis on the whole lifecycle of a device and a recommendation that manufacturers include a Software Bill of Materials (SBOM) with all new products that gives users information on the various elements that make up a device. An SBOM makes it easier for users to keep tabs on their devices. If there's a bug or vulnerability found in a bit of software, for example, a hospital could easily check if their infusion pumps use that specific software.

The FDA has put out legislative proposals around medical device cybersecurity, asking asking Congress for more explicit power to make requirements. “The intent is to enable devices to be that much more resilient to withstand the potential for cyber exploits or intrusion,” Schwartz says. Manufacturers should be able to update or patch software problems without hurting the devices' function, she says.

The FDA's efforts dovetail with a proposed bill introduced in Congress this week, the **Protecting and Transforming Cyber Health Care (PATCH) Act**, which would codify some of the FDA's proposals. The bill would require device manufacturers to have a plan to address any cybersecurity issues with their devices, and require an SBOM for new devices.

Lesson from Insteon:

IoT service shuts down its cloud hosts without warning; execs scrub their Linkedin profiles of the company's name; parent company deletes press-release trumpeting the acquisition, and every single device they've ever sold is bricked. (via Cory Doctorow twitter feed this week)

https://arstechnica.com/gadgets/2022/04/shameful-insteon-looks-dead-just-like-its-users-smart-homes/

Lesson from Omron:

Dragos pipe dream report (reiterated by DHS and NSA) indicates nation-state hacking against PLC’s in Omron and Schneider ICS products.

Chernovite’s Pipedream can execute 38 percent of known ICS attack techniques and 83 percent of known ICS attack tactics,” said Dragos. “It can manipulate a wide variety of industrial control programmable logic controllers (PLC) and industrial software, including Omron and Schneider Electric controllers, and can attack ubiquitous industrial technologies including CODESYS, Modbus, and Open Platform Communications Unified Architecture (OPC UA). Together, Pipedream can affect a significant percentage of industrial assets worldwide. It is not currently taking advantage of any Schneider or Omron vulnerabilities, instead it leverages native functionality.

Lesson from Cynerio:

An analysis of more than 200,000 infusion pumps from seven medical device manufacturers, using crowd-sourced data supplied by healthcare organizations, found more than half of the devices were susceptible to "critical" and "high" severity cybersecurity vulnerabilities. "Security lapses in these devices have the potential to put lives at risk or expose sensitive patient data," states the report, noting that infusion pumps can number in the thousands in a large hospital or clinic.

The Palo Alto Networks study mirrors results from a January research report by security firm Cynerio, which found that IV infusion pumps make up 38% of a hospital's typical Internet of Things (IoT) footprint, with 73% of those devices having a vulnerability "that would jeopardize patient safety, data confidentiality, or service availability if it were to be exploited by an adversary."

https://www.medtechdive.com/news/infusion-pumps-cyber-flaws-at-risk-hackers-bd-baxter/619735/

Some Recent CISA Medical Advisories

ICS Advisory (ICSA-22-067-01)
PTC Axeda agent and Axeda Desktop Server
https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01

BD Alaris infusion pumps - Linux kernel wifi issues

Biotronik CardioMessenger II - cleartext passwords

Medical ProdSec Resources

https://www.gehealthcare.com/security
https://www.siemens.com/industrialsecurity
https://www.baxter.com/product-security
https://www.abbott.com/corpnewsroom/strategy-and-strength/device-cybersecurity.html

Takeaways

1. Many parts of the government can contribute to the demands on medical devices: DHS, TSA, FDA, FCC, USDA, VA. The FDA may have a new mandate to enforce SBOM creation and maintenance so that at least the public can know what software device vendors have been using.

2. Industrial Control Systems requirements are often the closest guidance for improving security functionality while providing value through reduction of risks to availability (light bulbs). Currently vulnerabilities for medical devices are tracked in CISA's ICS area.

3. M&A integrations will push interoperability and better encryption and security development practices among device makers. Efforts to manage "device identities" for instance by Venafi may help to track affected devices.

4. Pharmaceuticals, hospital management and IT, MD and nursing staff, should all play a role in how the device changes occur by device manufacturers. SBOM creation is only a start.

5. Product security as a discipline is maturing and will make a tremendous and positive difference in the secure architecture and design of medical products, and will lead to faster and more accurate disclosure coordination, the operation of bug bounties, and streamlined workflows for getting security fixes out.

AVAILABILITY
INTEGRITY
CONFIDENTIALITY
NON-REPUDIATION