NIST SPECIAL PUBLICATION 1800-8A

Securing Wireless Infusion Pumps

in Healthcare Delivery Organizations

Volume A:
Executive Summary

Gavin O'Brien
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

August 2018

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8

The first draft of this publication is available free of charge from: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

- Broad technological advancements have contributed to the Internet of Things (IoT) phenomenon, where physical devices now have technology that allow them to connect to the internet and communicate with other devices or systems. With billions of devices being connected to the internet, many industries, including healthcare, have leveraged, or are beginning to leverage, IoT devices to improve operational efficiency and enhance innovation.
- Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other tools within a healthcare delivery organization (HDO)—ultimately contributing to the Internet of Medical Things (IoMT).
- As IoMT grows, cybersecurity risks have risen. According to the Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report 57 (TIR57), "this has created a new source of risk for [the] safe operation [of medical devices]." In particular, the wireless infusion pump ecosystem (the pump, the network, and the data stored in and on a pump) faces a range of threats, including unauthorized access to protected health information (PHI), changes to prescribed drug doses, and interference with a pump's function.
- In addition to managing interconnected medical devices, HDOs oversee complex, highly technical environments, from back-office applications for billing and insurance services, supply chain and inventory management, and staff scheduling, to clinical systems, such as radiological and pharmaceutical support. In this intricate healthcare environment, HDOs and medical device manufacturers that share responsibility and take a collaborative, holistic approach to reducing cybersecurity risks of the infusion pump ecosystem can better protect healthcare systems, patients, PHI, and enterprise information.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) analyzed risk factors in and around the infusion pump ecosystem by using a questionnaire-based risk assessment. With the results of that assessment, the NCCoE then developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

CHALLENGE

Technology improvements happen rapidly across all sectors. For organizations focused on streamlining operations and delivering high-quality patient care, it can be difficult to take advantage of the latest technological advances, while also ensuring that new medical devices or applications are secure. For many HDOs, this can result in improperly configured information technology networks and components that increase cybersecurity risks.

Unlike prior medical devices that were once standalone instruments, today's wireless infusion pumps connect to a variety of healthcare systems, networks, and other devices. Although connecting infusion pumps to point-of-care medication systems and electronic health records (EHRs) can improve healthcare delivery processes, using a medical device's connectivity capabilities can create significant cybersecurity risk, which could lead to operational or safety risks. Tampering, intentional or otherwise, with the wireless infusion pump ecosystem can expose a healthcare provider's enterprise to serious risks, such as the following examples:

- access by malicious actors
- loss or corruption of enterprise information and patient data and health records
- a breach of PHI
- loss or disruption of healthcare services
- damage to an organization's reputation, productivity, and bottom-line revenue

As IoMT grows, with an increasing number of infusion pumps connecting to networks, the vulnerabilities and risk factors become more critical, as they can expose the pump ecosystem to external attacks, compromises, or interference.

SOLUTION

The NCCoE has developed cybersecurity guidance, NIST Special Publication (SP) 1800-8: *Securing Wireless Infusion Pumps*, by using standards-based commercially available technologies and industry best practices to help HDOs strengthen the security of the wireless infusion pump ecosystem within healthcare facilities.

This NIST cybersecurity publication provides best practices and detailed guidance on how to manage assets, protect against threats, and mitigate vulnerabilities by performing a questionnaire-based risk assessment. In addition, the security characteristics of the wireless infusion pump ecosystem are mapped to currently available cybersecurity standards and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Based on our risk assessment findings, we apply security controls to the pump's ecosystem to create a "defense-in-depth" solution for protecting infusion pumps and their surrounding systems against various risk factors. Ultimately, we show how biomedical, networking, and cybersecurity engineers and IT professionals can securely configure and deploy wireless infusion pumps to reduce cybersecurity risk.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide to securing wireless infusion pumps in HDOs can help your organization:

- reduce cybersecurity risk, and potentially reduce impact to safety and operational risk, such as the loss of patient information or interference with the standard operation of a medical device
- develop and execute a defense-in-depth strategy that protects the enterprise with layers of security to avoid a single point of failure and provide strong support for availability

- implement current cybersecurity standards and best practices, while maintaining the performance and usability of wireless infusion pumps

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/medical-devices. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hit_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

B|BRAUN Baxter BD cisco CLEARWATER COMPLIANCE digicert Hospira intercede

MDISS PFP CYBERSECURITY RAMPARTS smiths medical bringing technology to life Symantec TD

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200