Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

12 September 2022

PIN Number

20220912-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities

Summary

The FBI has identified an increasing number of vulnerabilities posed by unpatched medical devices that run on outdated software and devices that lack adequate security features. Cyber threat actors exploiting medical device vulnerabilities adversely impact healthcare facilities' operational functions, patient safety, data confidentiality, and data integrity. Medical device vulnerabilities predominantly stem from device hardware design and device software management. Routine challenges include the use of standardized configurations, specialized configurations, including a substantial number of managed devices on the network, lack of device embedded security features, and the inability to upgrade those features.

Threat

Medical device hardware often remains active for 10-30 years, however, underlying software life cycles are specified by the manufacturer, ranging from a couple months to maximum life expectancy per device allowing cyber threat actors time to discover and exploit vulnerabilities. Legacy medical devices contain outdated software because they do not receive manufacturer support for patches or updates, making them especially vulnerable to cyber attacks.

In addition to outdated software, many medical devices also exhibit the following additional vulnerabilities:

- Devices used with the manufacturer's default configuration are often easily exploitable by cyber threat actors.
- Devices with customized software, require special upgrading and patching procedures, delaying the implementation of vulnerability patching.
- Devices not initially designed with security in mind, due to a presumption of not being exposed to security threats.

Medical devices have known vulnerabilities that impact various machines used for healthcare purposes, including those that sustain patients with mild to severe medical conditions.

- As of January 2022, a research report conducted by a cybersecurity firm found 53% of connected medical devices and other internet of things (IoT) devices in hospitals had known critical vulnerabilities. Approximately one third of healthcare IoT devices have an identified critical risk potentially implicating technical operation and functions of medical devices.
- According to a report in mid-2022 conducted by a healthcare cybersecurity analyst, medical devices that are susceptible to cyber attacks include insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers, and intrathecal pain pumps. Malign actors who compromise these devices can direct them to give inaccurate readings, administer drug overdoses, or otherwise endanger patient health.
- According to a research report in 2021, a cybersecurity firm assessed there is an average of 6.2 vulnerabilities per medical device, and recalls were issued for critical devices such as pacemakers and insulin pumps with known security issues, while more than 40% of medical devices at the end-of-life stage offer little to no security patches or upgrades.

Recommendations

The FBI recommends considering the following to actively secure medical devices, identify vulnerabilities, and increase employee awareness reporting in order to help mitigate the risk posed by medical devices.

- Endpoint Protection
  - If supported by the medical device, use antivirus software on an endpoint. If not supported, providing integrity verification whenever the device is disconnected for service and before it is reconnected to the IT network.
  - Encrypt medical device data while in transit and at rest.
  - Utilize endpoint detection and response (EDR) and Extended Detection and Response (XDR) solutions, which provides visibility on medical devices and offers protection.
- Identify and Access Management
  - Ensure default passwords are changed to secure and complex passwords specific for each medical device. If supported by medical device, limit the number of login attempts per user.
- Asset Management
  - Maintain an electronic inventory management system for all medical devices and associated software, including vendor-developed software components, operating systems, version and model numbers.
  - Use inventory results to identify critical medical devices, operational properties, and maintenance timeframes.
  - Consider replacement options for affected medical devices as part of purchasing process; if replacing the medical device is not feasible, take other mitigation precautions, such as isolating the device from network or auditing the device's network activities.
- Vulnerability Management
  - Work with manufacturers to help mitigate vulnerabilities on operational medical devices.
  - Monitor and review medical devices' software vulnerabilities disclosures by vendors and conduct independent vulnerability assessments.
  - Implement a routine vulnerability scan before installing any new medical device onto the operating IT network.

- Training to Help Mitigate Risk Associated with Employees
    - Implement required training for employees on how to identify and report potential threats:
        - Insider threats related to employees seeking to cause harm to the network or steal information. This includes training on the types of behavior and activity to look for.
        - Attacks targeting employees including phishing, social engineering, and spoofing attempts to compromise their accounts or credentials.
        - As budget constraints allow consider email alert banners for all email exchanges originating outside of the organization.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.