CYBLE®

Vulnerability Management in Healthcare IoT Devices:

Best Practices for Securing Medical Equipment

CONTENTS

INTRODUCTION

The Digital Dilemma: Securing Healthcare IoT Devices

In the era of digital transformation, healthcare has not been an exception. The integration of Internet of Things (IoT) devices into medical infrastructure, often referred to as Internet of Medical Things (IoMT), has revolutionized patient care and operational efficiency. However, this technological advancement has also introduced a new set of security challenges. As these devices become increasingly interconnected, they present malicious actors with a vast attack surface for exploitation.

These devices, ranging from insulin pumps to MRI machines, often lack robust security features, making them vulnerable to a variety of cyber threats.

The challenges and risks associated with vulnerabilities in healthcare IoT devices are significant. Compromised IoMT devices can lead to data breaches, disruption of medical services, adverse reputational damage, and financial losses, including cleanup costs, fines, legal expenses and lost revenue.

This report delves into the critical issues surrounding vulnerability management in healthcare IoT devices, examining prevalent threats, their devastating consequences, and indispensable strategies for safeguarding sensitive patient data and ensuring the integrity of medical operations.

FACTS AND FIGURES THAT MAKE THE CASE

The data paints a picture of a highly vulnerable IoMT infrastructure.

1. DDoS Attacks

- **Increase:** Distributed Denial of Service (DDoS) attacks on IoT surged by 300% in the first half of 2023.
- **Financial Impact:** These attacks caused global financial losses of $2.5 billion.

2. Malware Attacks

Increase: IoT malware attacks increased by 400%.

3. Unpatched Security Flaws

Infusion Pumps: 75% of infusion pumps have unpatched security flaws.

4. Unsupported Operating Systems

Medical Imaging Systems: 83% of medical imaging systems run on unsupported operating systems.

5. Unencrypted Network Traffic

98% of IoMT device network traffic is unencrypted.

6. Healthcare Data Breaches

- **88%** of healthcare organizations experienced at least one data breach in the past two years due to a vulnerability in a connected device.
- **Average Cost:** The average cost of a healthcare data breach in 2023 was $10.93 million, the highest among all industries.
- **Increase:** Since 2020, the cost of a data breach in healthcare has increased by 53.3%.

7. Device Exposure

Over 50% of hospital IoT devices are vulnerable to attack.

8. Ransomware Attacks on Healthcare

- **Observation:** Cyble's researchers have observed that Ransomware attacks, such as from the notorious Qilin and Rhysida ransomware groups, have significantly impacted healthcare organizations, demanding huge ransoms to unlock vital systems and crippling operations.
- IoMT devices were the root cause of 21% of all ransomware attacks in the healthcare sector.
- **Ransomware attacks on healthcare organizations have led to:**
  - Longer stays at the hospital for patients.
  - Poor patient outcomes caused by delays in tests and procedures.
  - Increase in patient transfers and medical complications.
  - Increase in mortality rate.

9. Vulnerable Medical Information Systems

Medical information systems that store and manage clinical data are often exposed online, making them susceptible to attacks.

10. Security Audits

Only 52% of companies conduct regular security audits for healthcare IoT devices.

KEY TAKEAWAYS

High Incidence of Data Breaches
The overwhelming majority of healthcare organizations have experienced data breaches due to vulnerabilities in IoT and IoMT devices.

Ransomware Prevalence
Ransomware attacks are a significant threat, with many healthcare organizations experiencing multiple attacks.

Unpatched Devices
A substantial portion of IoT devices in healthcare, such as infusion pumps and medical imaging systems, have unpatched vulnerabilities.

Lack of Encryption
The vast majority of IoT device network traffic remains unencrypted, posing severe risks for data interception.

Patient Care Impact
Cyberattacks, particularly ransomware, have direct adverse effects on patient care, including increased mortality rates.

Infrequent Security Audits
Less than half of healthcare organizations regularly conduct security audits for their IoT devices.

UNDERSTANDING VULNERABILITIES IN HEALTHCARE IoT/IoMT DEVICES

While both traditional IoT and IoMT devices share some common vulnerabilities, the unique characteristics of IoMT devices, such as data sensitivity, interoperability, and real-time requirements, introduce specific challenges that require tailored security measures.

Vulnerabilities in healthcare IoT/IoMT devices can be broadly divided into four types:

1. Software Vulnerabilities

A report from the Health Information Sharing and Analysis Center (Health-ISAC) revealed that software applications used in the healthcare sector account for the highest percentage (64%) of vulnerabilities found.

- **Buffer Overflow:** Errors that occur when data exceeds a buffer's storage capacity, leading to data corruption and potential code execution.
- **Insecure APIs:** Flaws in application programming interfaces (APIs) can be exploited to gain unauthorized access or leak sensitive data.
- **Unpatched Software:** Failure to apply security patches can leave systems vulnerable to known exploits – and outdated or unsupported operating systems in IoMT devices can mean that patching may not be possible, requiring other mitigations.

2. Hardware Vulnerabilities

Hardware vulnerabilities were the second largest group, with 27% of vulnerabilities.

- **Insecure Firmware:** Flaws in the device firmware that can be exploited to gain control over the device.
- **Side-Channel Attacks:** Attacks that exploit physical characteristics of the hardware, such as power consumption or electromagnetic leaks.
- **Hardware Backdoors:** Malicious or unintended backdoors in hardware components.

UNDERSTANDING VULNERABILITIES IN HEALTHCARE IoT/IoMT DEVICES

3. Network Vulnerabilities

- **Man-in-the-Middle (MitM) Attacks:** Attackers intercept and potentially alter communications between devices.
- **Insecure Communication Protocols:** Use of outdated or insecure protocols (e.g., HTTP instead of HTTPS).
- **Denial of Service (DoS):** Overwhelming a network with traffic to disrupt services.

4. Configuration Vulnerabilities

- **Default Credentials:** Use of factory default usernames and passwords, making devices easy targets.
- **Improper Access Controls:** Weak or insufficient access controls that allow unauthorized users to access sensitive areas or data.
- **Misconfigured Network Settings:** Incorrect network settings that expose devices to the internet or other unauthorized networks.

MOST COMMON ATTACK TYPES OBSERVED IN HEALTHCARE IoT/IoMT DEVICES

Here are some of the most common recent attack types that have resulted from vulnerabilities in healthcare IoT devices.

Remote Code Execution (RCE)

Attackers exploit software vulnerabilities to execute arbitrary code on the device remotely. This can lead to an attacker taking full control over the device.

Example: CISA recently added CVE-2023-43208 to its Known Exploited Vulnerabilities (KEV) catalogue on May 20, 2024. This bug in NextGen Healthcare Mirth Connect allowed unauthenticated remote code execution. Mirth Connect is an open-source data integration platform widely used by healthcare companies to manage information using bi-directional flow of various message types. Attackers could exploit this vulnerability for initial access or to compromise sensitive healthcare data.

Unauthorized Access

Gaining access to devices or networks without proper authorization, often due to weak authentication mechanisms.

Example: GE Healthcare and the ICS-CERT/CISA warned of a vulnerability that arose from connecting a device serial port via an add-on and an insufficiently secured third-party terminal server to a hospital network. The bug allowed unauthorized access to certain GE Healthcare's GE Aestiva and Aespire anesthesia devices.

Firmware Exploits

Exploiting vulnerabilities in the device firmware to gain control or disrupt operations.

Example: A set of bugs related to a particular firmware version used in the Sigma infusion pump manufactured by Baxter and several versions of its associated WiFi batteries.

Data Breaches

Unauthorized access to sensitive patient data, often through network vulnerabilities or unsecured storage.

Example: Intercepting unencrypted data transmitted between a medical device and its control system.

LIST OF MOST VULNERABLE MEDICAL DEVICES

These are some of the most vulnerable devices to cyberattacks. It's important to understand the specific vulnerabilities and implications of attacks on these devices, which play a crucial role in patient care.

Insulin Pumps

- **Description:** Small, computerized devices that deliver insulin to diabetic patients in controlled doses.
- **Vulnerabilities:** Weak encryption, unsecured wireless communication.
- **Attack Methods:** Intercepting and altering insulin dosage instructions.
- **Impact:** Can lead to severe hypo- or hyperglycemia.
- **Documented Incidents:** Researchers have demonstrated the ability to control insulin pumps and alter dosing levels remotely.

Implantable Cardiac Devices (Pacemakers)

- **Description:** Devices implanted in the chest to help control abnormal heart rhythms.
- **Vulnerabilities:** Susceptible to wireless signal interception and reprogramming.
- **Attack Methods:** Hacking to change heart rhythms, stop functioning, or drain batteries.
- **Impact:** Can cause cardiac arrest or other serious cardiac events.
- **Documented Incidents:** Security researchers have observed vulnerabilities in several pacemaker models that could be exploited.

Infusion Pumps

- **Description:** Devices used to deliver fluids, including medications, at a set rate.
- **Vulnerabilities:** Network connection breaches.
- **Attack Methods:** Altering drug formulas, dosages, or infusion rates.
- **Impact:** Risk of drug overdose or underdose.
- **Documented Incidents:** The FDA has issued warnings about specific infusion pump models vulnerable to hacking.

Patient Monitors

- **Description:** Devices that continuously monitor and display vital signs like heart rate and blood pressure.
- **Vulnerabilities:** Data transmission interception/manipulation.
- **Attack Methods:** Falsifying vital sign data.
- **Impact:** Misdiagnosis or delayed treatment.
- **Documented Incidents:** Hacking demonstrations have shown potential for manipulating patient monitor data.

LIST OF MOST VULNERABLE MEDICAL DEVICES

Diagnostic and Imaging Equipment

- **Description:** Includes CT scanners, ultrasound machines, and other diagnostic tools.
- **Vulnerabilities:** Susceptible to hacking and providing false diagnostic information.
- **Attack Methods:** Manipulating imaging results.
- **Impact:** Leads to incorrect treatment decisions.
- **Documented Incidents:** Generally, vulnerabilities are known, but direct attacks are less common.

MRI Machines

- **Description:** Advanced imaging devices are used to visualize the body's internal structures.
- **Vulnerabilities:** Software/hardware disruption.
- **Attack Methods:** Introducing malware or system breaches.
- **Impact:** Incorrect imaging results.
- **Documented Incidents:** While direct attacks are rare, MRI machines are often impacted in broader healthcare cyber-attacks.

Surgical Robots

- **Description:** Robotic systems used for performing precise, minimally invasive surgeries.
- **Vulnerabilities:** Dependence on precise control and network connectivity.
- **Attack Methods:** Loss of control or manipulation of movements.
- **Impact:** Potential for surgical errors.
- **Documented Incidents:** Researchers have demonstrated theoretical vulnerabilities, though actual incidents are rare.

Radiation Therapy Systems

- **Description:** Equipment used for cancer treatment by delivering radiation to target areas.
- **Vulnerabilities:** Software manipulation.
- **Attack Methods:** Altering radiation dosage levels.
- **Impact:** Incorrect radiation doses can harm patients.
- **Documented Incidents:** Specific vulnerabilities have been identified, though no direct attacks are publicly known.

LIST OF MOST VULNERABLE MEDICAL DEVICES

Defibrillators

- **Description:** Emergency devices used to deliver a dose of electric current to the heart.
- **Vulnerabilities:** Hacking to disrupt shocks or battery depletion.
- **Attack Methods:** Preventing the device from functioning in emergencies.
- **Impact:** Life-threatening if not available during cardiac emergencies.
- **Documented Incidents:** Vulnerabilities in certain models have been exposed, but no attacks have been reported.

Hospital Networking Equipment

- **Description:** The backbone of a hospital's IT infrastructure, connecting various medical devices.
- **Vulnerabilities:** Network breaches can lead to widespread dysfunction.
- **Attack Methods:** Gaining unauthorized access to the network, affecting connected devices.
- **Impact:** Loss of critical patient data, malfunctioning of medical devices.
- **Documented Incidents:** Various healthcare networks have been victims of cyberattacks, leading to significant disruptions – with a recent noteworthy example the Synnovis ransomware attack that impacted blood sampling in major London hospitals.

MOST TARGETED VULNERABILITIES IN MEDICAL DEVICES

While new vulnerabilities in healthcare IoT/IoMT devices are observed nearly on a weekly basis, Cyble's Research and Intelligence Labs has observed the following CVEs as the most targeted vulnerabilities during the reporting period

- **CVE-2022-22766:** Affecting Becton, Dickinson, and Company (BD) devices.
- **CVE-2021-27410:** Affecting Hillrom devices.
- **CVE-2018-14786:** Affecting Becton, Dickinson, and Company (BD) devices.
- **CVE-2018-4846:** Affecting Siemens AG devices.
- **CVE-2021-27408:** Affecting Hillrom devices.
- **CVE-2021-32025:** Affecting Blackberry devices.
- **CVE-2018-4845:** Affecting Siemens AG devices.
- **CVE-2017-14006:** Affecting GE Healthcare devices.
- **CVE-2016-8355:** Affecting Smiths Medical – ICU Medical devices.
- **CVE-2021-22156:** Affecting Blackberry devices.

IMPACT OF VULNERABILITIES ON PATIENT SAFETY AND PRIVACY

Patients are, of course, the reason healthcare cyberattacks can be so damaging. Here are some of the ways patients can be harmed by cyberattacks.

Patient Safety

- **Medical Device Malfunctions:** Exploits can lead to device malfunctions, such as incorrect drug dosages or improper operation of life-support systems.
- **Delayed Care:** Ransomware or DoS attacks can disrupt hospital operations, delaying critical care.
- **Physical Harm:** Direct manipulation of medical devices can result in physical harm or even fatalities.

Patient Privacy

- **Exposure of Personal Health Information (PHI):** Data breaches can expose sensitive health information, including medical histories and social security numbers, which are highly valuable on the dark web.
- **Loss of Trust:** Repeated breaches can erode patient trust in the healthcare system, potentially leading to reluctance in sharing necessary health information.

Operational Impact

- **Financial Losses:** Costs associated with data breaches, including fines, legal fees, and remediation costs, can be substantial.
- **Reputation Damage:** Publicized breaches can damage the reputation of healthcare providers and reduce patient confidence.

UNITEDHEALTH CASE STUDY

An apt case study to understand how patient safety and privacy is impacted due to healthcare breaches and their huge financial consequences is the recent UnitedHealth breach that impacted millions of Americans.

Overview

- UnitedHealth Group suffered massive ransomware attack on February 12, from BlackCat (aka ALPHV).
- 6TB of healthcare records stolen, including PHI and PII of millions.
- Group's subsidiary, Change Healthcare's servers encrypted.
- Ransom of $22M demanded to prevent data leak.

Short-term Impact

- Encrypted servers severely crippled care providers daily routine.
- Attack delayed reimbursements, patient access to medications, and led to significant financial strains on healthcare providers.
- Some resorted to filing paper claims, incurring additional expenses.
- Smaller hubs faced existential cash-flow crises.

Response and Financial Impact

- UnitedHealth struggled to restore encrypted servers due to inadequate backup practices.
- UnitedHealth paid nearly $22 million in Bitcoin to the BlackCat group to prevent leakage of stolen data.
- Incident led to substantial recovery costs, with an estimated $1.6 billion spent as of May 2024.
- Its Q1 earnings were impacted by $872 million due to the cyberattack.
- Company offered credit monitoring and identity theft protection services and set up a dedicated support center.
- Analysts estimate UnitedHealth will spend another $1.6 billion in 2025 on related expenses, none of which will be covered by cyber insurance.

BEST PRACTICES FOR IoMT VULNERABILITY MANAGEMENT

Device Inventory and Management

- Accurate Device Inventory: Maintaining an accurate inventory of medical devices is crucial. This includes details like the operating system and software versions. Without this, making proper risk-based decisions is nearly impossible.
- Regular Updates and Patches: Ensuring that all devices receive regular updates and patches is essential for mitigating vulnerabilities, particularly in legacy systems that might no longer receive manufacturer support.

Security Measures and Protocols

- Encryption and Multi-Factor Authentication (MFA): Protecting cloud environments and network connections with encryption and MFA can significantly reduce the risk of unauthorized access.
- Network Segmentation: Separating sensitive data through network segmentation minimizes the risk of data breaches, a particularly important control for unsupported devices.

Utilization of AI and Automated Tools

AI for Threat Detection: Leveraging AI to identify and respond to security risks in real-time can enhance the security posture of healthcare IoT environments.

Compliance and Standards

- Compliance with Regulations: Adhering to healthcare regulations like HIPAA ensures that security measures are up to date and comprehensive.
- Utilization of Security Frameworks: Implementing frameworks such as those provided by OWASP and NIST can guide healthcare organizations in mitigating vulnerabilities.

Risk-Based Vulnerability Management (RBVM)

Prioritization of Vulnerabilities: By focusing on vulnerabilities that are most likely to be exploited, healthcare organizations can more effectively manage their security risks.

Monitoring and Response

Managed Detection and Response (MDR): Utilizing MDR services to monitor and respond to threats ensures that any anomalies in the network are investigated and addressed promptly.

EMERGING TRENDS AND TECHNOLOGIES

Here are some of the emerging practices, guidance and technologies that can help healthcare organizations improve IoMT security.

IoT Security Frameworks and Standards

These are essential for ensuring the safety and reliability of healthcare IoT and IoMT devices. These frameworks and standards provide guidelines and best practices for securing medical devices and the data they handle. Key aspects include:

- **Data Encryption:** Ensuring that all data transmitted between devices and servers are encrypted to prevent unauthorized access.
- **Authentication and Authorization:** Implementing strong authentication mechanisms to confirm the identity of users and devices, and ensuring they have the appropriate access rights.
- **Regular Software Updates and Patching:** Keeping device firmware and software up to date to protect against vulnerabilities.
- **Compliance with Regulations:** Adhering to healthcare regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the U.S., which mandates the protection of patient data.

Examples of Frameworks and Standards:

- **NIST (National Institute of Standards and Technology) Cybersecurity Framework:** Provides a policy framework for private sector organizations to assess and improve their ability to prevent, detect, and respond to cyberattacks.
- **ISO/IEC 27001:** Specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system.

AI and ML for Vulnerability Detection and Mitigation

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being used to enhance the security of healthcare IoT and IoMT devices:

- **Anomaly Detection:** AI and ML algorithms can analyze large volumes of data from IoMT devices to identify unusual patterns that may indicate a security threat.
- **Predictive Analytics:** ML models can predict potential vulnerabilities based on historical data and trends, allowing for proactive mitigation measures.
- **Automated Incident Response:** AI-driven systems can automate responses to security incidents, such as isolating compromised devices to prevent the spread of malware.

Use Cases for AI and ML:

- **Real-time Monitoring:** Continuous monitoring of device behavior to detect and respond to threats in real time.

EMERGING TRENDS AND TECHNOLOGIES

- **Threat Intelligence:** Leveraging ML to analyze global threat data and provide actionable insights for healthcare providers.

Blockchain for Secure Data Sharing and Authentication

Blockchain technology offers a decentralized and tamper-proof way to handle data, which is particularly valuable in the healthcare sector:

- **Data Integrity:** Blockchain ensures that medical data is immutable and traceable, which is crucial for maintaining the integrity of patient records.
- **Secure Data Sharing:** Enables secure and transparent sharing of medical data across different healthcare providers while maintaining patient privacy.
- **Authentication:** Blockchain can be used for verifying the identity of devices and users, reducing the risk of unauthorized access.

Blockchain applications:

- **Electronic Health Records (EHRs):** Securely storing and sharing patient records on a blockchain to enhance interoperability and security.
- **Supply Chain Management:** Using blockchain to track the provenance and authenticity of medical supplies and devices.

Edge Computing for Decentralized Security

Edge Computing involves processing data closer to the point of origin (e.g., IoMT devices) rather than relying solely on centralized or cloud servers:

- **Reduced Latency:** By processing data locally, edge computing reduces the time it takes to detect and respond to security threats.
- **Enhanced Privacy:** Sensitive data can be processed and analyzed locally, minimizing the risk of exposure during transmission.
- **Scalability:** Edge computing allows for more scalable security solutions, as it distributes the processing load across multiple nodes.

Edge computing benefits

- **Real-time Threat Detection:** Faster detection and response to security incidents due to the proximity of data processing.
- **Resilience:** Enhanced system resilience by distributing computing resources, reducing the impact of a single point of failure.

CONCLUSION

An Imperative for Proactive Security

The vulnerability landscape for healthcare IoT/IoMT devices is evolving at a breakneck pace, demanding a proactive and comprehensive approach to security. The findings presented in this report are evidence of the urgent need for healthcare organizations to prioritize vulnerability management and implement robust security measures.

By adopting best practices such as device inventory and management, network segmentation, encryption, and regular security audits, healthcare providers can significantly reduce the risk of cyberattacks and protect the sensitive data of their patients.

Moreover, the emergence of technologies like AI, cyber threat intelligence, blockchain, and edge computing offers promising solutions for enhancing the security of healthcare IoT environments. Embracing these innovations can equip healthcare organizations with the tools necessary to stay ahead of evolving threats and ensure the safety and reliability of their medical infrastructure.

In conclusion, the security of healthcare IoT devices is paramount for protecting patient safety, privacy, and the overall integrity of the healthcare system. By understanding the prevalent vulnerabilities, their devastating consequences, and best practices for mitigation, healthcare organizations can take a proactive stance in safeguarding their digital assets and ensuring the continued delivery of high-quality care for patients.

To enable a program of proactive vulnerability management, healthcare organizations should adopt intelligent AI-driven vulnerability management solutions like Cyble's.

Cyble's vulnerability management database is not only fully aligned with the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD), but also provides in-depth information on a significant number of issues that go unreported by the CVE and NVD systems. With Cyble, healthcare organizations can gain access to extensive metadata, including information on exploits, methods of attack, and solutions.

To learn more about how Cyble can help your healthcare organization solve the vulnerability management problem, schedule a demo today!

Industry Recognition

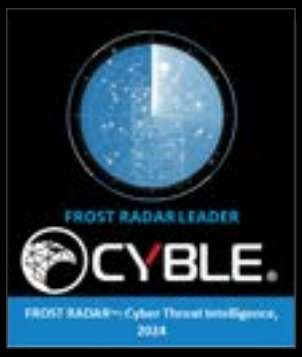
Gartner®

Cyble Named a Sample Vendor in Three Gartner® Hype Cycles for Managed IT Services, 2024, Cyber Risk Management, 2024 and Security Operations, 2024

FORRESTER®

Cyble Recognized in Forrester's Attack Surface Management Solutions Landscape Q2-2024 Report

FROST & SULLIVAN



Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Gartner Peer Insights™

4.6/5

Ranked among top 5 cyber threat intelligence providers

Named a leader in the G2 Grid for Dark Web Monitoring

Named Editor's Choice for Threat Intelligence by Cyber Defense Magazine

Earned nine awards at the Global InfoSec Awards during RSA

Ranked in Y Combinator's Top 100 AI Startups for 2024

Recognized as one of America's Best Startup Employers by Forbes

CYBLE®

Cyble provides one of the fastest and most comprehensive coverages across adversaries, infrastructure, exposure, weaknesses, and targets by leveraging cutting-edge AI technology and real-time threat intelligence and detection. Through advanced data analysis, expert insights, and automated processes, Cyble facilitates swift detection, prioritization, and remediation of security threats, and enables governments and enterprises to protect their citizens and infrastructure by delivering crucial intelligence promptly. Headquartered in Atlanta, GA, and with employees across 12 countries, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com

11175 Cicero Drive Suite, 100 Alpharetta GA 30022, US. | contact@cyble.com | +1 888 673 2067