Managing Medical Device Vulnerabilities Efficiently

Matt Dimino, CISM, CRISC, HCISPP, CEH
EVP & CSO
First Health Advisory

Jessica Pitterka, CSM, CSPO
Clinical Asset Defense Engineer
HonorHealth

May 05, 2022
ACCE gratefully acknowledges the sponsorship of this webinar by FIRST HEALTH ADVISORY.
About the Moderator

Angelina Chiaracane, MS, CABT
Kaiser Permanente
Clinical System Engineer
Member, ACCE Education Committee

Angelina is a Clinical System Engineer at Kaiser Permanente in Northern California responsible for the implementation of equipment and capital projects. She is actively working on converting the entire fleet of large volume infusion pumps for the Region. Previously she has served as a Clinical Technology Manager and developed standardization practices and documentation for service delivery.

Angelina received her Bachelor’s in Bioengineer from Florida Gulf Coast University, received her Master’s Degree in Clinical Engineering from the University of Connecticut.
Logistics

• All attendees have their microphones muted during the presentation.

• Questions to the panelists must be submitted via the “Q&A” feature (not chat) in Zoom at any time.

• We will try to ask Matt and Jessica to answer questions not addressed during the webinar and distribute them to participants via email or post them to ACCE website.

• Please remember to complete the webinar evaluation after attending. A link will be provided at the end.
About the speaker

Matt Dimino
EVP & Chief Security Officer
Clinical & Operational Technology

Matt brings a wide range of technical, security, and HTM knowledge to this role. Matt has over 15 years’ experience in various HTM roles from senior technical to leadership roles and 5 of those years as a practitioner in medical device security. Throughout his career he has developed multiple security programs, integrated complex architectures, performed security consulting, as well as developed IoMT risk assessment methodologies.
Jessica Pitterka is tenured Medical Device Security Engineer currently working at HonorHealth with over five years of security experience with the healthcare industry. As a Clinical Asset Defense Engineer, she is pivotal in driving medical device security initiatives, managing security projects, and provides guidance to healthcare technology procurements and assessments. Jessica is a Certified Scrum Product Owner and ScrumMaster.
Effective vulnerability management for medical devices requires organizations to understand how to assess risk and prioritize their mitigation activities within the context of the threats to the devices in their specific environment. Organizations must first understand their environment by having high fidelity visibility, assets appropriately identified and fingerprinted, and an understanding of device criticality and sensitivity from a business and patient impact perspective.

Efficient vulnerability management works when teams utilize more than just security tools to identify and triage applicable vulnerabilities, they have a collaborative, well-documented risk management approach, track their efforts, and prioritize based on defined factors conducive to their program.
Why Vulnerability Management?

- Increased organizational risk
- Safety – patients & organization
- Compliance – regulatory requirements and internal policies
- To understand the impacts of breaches and security incidents
- Increase in HDO targeted attacks

Understanding the risk
### IoMT Risk

#### Your Challenge

- CISA notifications, industry alerts, and IoMT passive scanning tools are revealing an overwhelming amount of vulnerabilities
- Increases in organizational risk, and it’s unclear how to manage
- Organizations are struggling with how to prioritize vulnerabilities for remediation

#### Common Obstacles

- Patches are rarely an applicable solution
- Many don’t understand that vulnerabilities for IoMT devices exist beyond CVE’s
- Organizations are unaware of the risk implications and lack the insight to remediation options

#### Approach

- Design and implement a risk management program
- Understand all factors when implementing remediation options
- Build a strategy from a framework

---

**Vulnerability Management**  
=  
**Patch Management**
Your Challenge

CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page.

https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
Common Obstacles and Misconceptions

- HTM must “patch everything”
- Vulnerability management is underappreciated
- Vulnerability management as part of Patch management
- Misalignment between HTM, SecOps, and ITOps
Approach

**Identify Vulnerability Sources**
- **Identify** Inventory & know your vulnerability threat intelligence data sources.
- **Define** roles & responsibilities ahead of time.

**Triage & Prioritize**
- **Contextualize** vulnerabilities based on your security posture.
- **Identify and assign risk**
- **Vendor** Contact (workflow and process) approval & Cadence

**Remediate Vulnerabilities**
- **Address** the vulnerabilities based on their level of risk.
- **Patching** isn’t the only option
- **Reduce** the risk down to medium/low levels and engage your regular operational processes to deal with the latter

**Measure & Formalize**
- **Measure** with metrics to ensure that the program is successful.
- **Track** your efforts within the CMMS/CMDB & IoMT tool
- **Ensure** continuous improvement.
Vulnerability Management: A Risk-Based Approach

1 Identify

Identify vulnerabilities from IoMT passive scanning tool & external threat sources (US-Cert, vendor alerts, Mitre, NIST)

2 Analyze

Assign risk (impact x urgency) to the organization based on current security posture

3 Assess

Plan risk mitigation strategy

Consider:
- Risk tolerance
- Patient impact
- Business impact
- Compensating controls

A risk matrix is useful in calculating a risk rating for vulnerabilities.
The Truth:

77% of CVE’s have no published or observed exploit.
Phase 1: Identify Vulnerability Sources

**Phase 1**
- What is vulnerability management?
- Define scope and roles
- Vulnerability detection

**Phase 2**
- Triage vulnerabilities
- Determine business criticality
- Consider current security posture
- Risk assessment of vulnerabilities

**Phase 3**
- Assessing remediation options
- Scheduling and completing remediation
- Continuous improvement

**Phase 4**
- Metrics, KPIs & CSFs
- Vulnerability management policy
- SLA’s
What is Vulnerability Management?

• Vulnerability management in IoMT is the ongoing practice of passively scanning your environment of care to uncover vulnerabilities:
  • Outdated applications
  • Unpatched operating systems and software
  • Open/unnecessary ports
  • Obsolete hardware
  • Anomalies and poor habits
Effective Vulnerability Management

- Effectiveness requires a formal process
- Patching isn’t the only solution, but it’s the one that often draws focus
- Responsibilities need to be defined
- Identifying new threats without proper passive scanning tools can be a near-impossible task
- Determining which vulnerabilities are most urgent is necessary for effectiveness
- Measuring the effectiveness of your vulnerability remediation activities can help you better manage resources
Determine Scope of Your VM Program

• Scope can be defined along with four aspects:
  • Asset Scope
  • Physical Scope
  • Organizational Scope
  • CE/HTM/IT/IS Scope
IoMT Assets Within Scope

• An up-to-date and comprehensive asset inventory for vulnerability management is critical
  • Vulnerabilities need to be compared to an inventory to determine if the organization has any relevant systems or versions.
  • It indicates where IoMT assets can be found both physically and logically.
  • Asset inventories typically have owners assigned to the assets and systems whose responsibility is to carry out remediations for vulnerabilities.
Inventory Must Include Software & Applications

• All connected device asset attributes should be accounted for

• Not all vulnerabilities are specific to a device/platform, they can be specific to a software library associated with a device (Java, Adobe, etc)

Tactical Insight

Requesting SBOM to identify the libraries associated with your device inventory
Assign Roles and Responsibilities for VM

• IS/Risk Mgmt to identify the true organizational risk
• Remediation can include implementing compensating controls, system and application hardening, or segmentation.
  • Who carries out each of these activities? Who coordinates the activities and tracks them to ensure completion?
• The people involved may be IT Ops, infrastructure, and Apps
Phase 2: Triage and Prioritize

Phase 1
- What is vulnerability management?
- Define scope and roles
- Vulnerability detection

Phase 2
- Triage vulnerabilities
- Determine business criticality
- Consider current security posture
- Risk assessment of vulnerabilities

Phase 3
- Assessing remediation options
- Scheduling and completing remediation
- Continuous improvement

Phase 4
- Metrics, KPIs & CSFs
- Vulnerability management policy
- SLA’s
Triage Vulnerabilities

- Triaging is an important step in vulnerability management
- IoMT passive scanning tools provide threat intel and cross-reference vulnerabilities with your inventory

Tactical Insight

IoMT security tool needs to be tuned, validated, and configured correctly
Determine Urgency

• Is there an exploit in the wild?
• What is the CVSS base score?
• Is there potential for significant lateral movement?
• Is there potential for patient harm?
• What is the impact to the organization
Determine Business Criticality

• Could the risk cause significant business disruption?
• Could the risk cause significant financial loss?
• Could the risk cause reputational damage?
• Would the organization go on diversion with the loss of the asset?
Review Current Security Posture

• Your IoMT scanning tool alone may not have the context needed for your security posture

• Enterprise architecture (firewalls, ACLS, VLANS) should be factored into determining risk of a vulnerability

• Current security posture will contribute to the assessment and remediation/mitigation options
Vulnerability Prioritization Example

EternalBlue CVSS – 8.1 v3
Actively being exploited
Remote execution
Business critical
Life critical assets affected

Real score: 9

Urgent/11 CVSS – 9.8 v3
Not actively being Exploited
Remote/Local execution
Business critical
Life critical assets affected

Real Score: 4
Vulnerabilities and Risk

• Vulnerabilities are a risk to patients and the business
• Your organization likely has a risk tolerance level that defines the organization’s risk appetite (measure of dollars, patient safety, productivity, down-time, etc)
• The risk of a vulnerability can be determined by impact and likelihood.
A Risk-based Approach to Vulnerability Management

• Vulnerabilities are never-ending
• You won’t be able to resolve all vulnerabilities
• IoMT security tools share CVSS scores but do not understand all of the controls you may have in place (compensating controls, device hardening)
• Determining actual risk is a crucial step
Phase 3

Phase 1
- What is vulnerability management?
- Define scope and roles
- Vulnerability detection
- Shape procedures

Phase 2
- Triage vulnerabilities
- Determine business criticality
- Consider current security posture
- Risk assessment of vulnerabilities

Phase 3
- Assessing remediation options
- Scheduling and completing remediation

Phase 4
- Metrics, KPIs & CSFs
- Refine Procedures
- Vulnerability management policy
- SLA’s
Assessing Remediation Options

• Build out the specific processes for remediating vulnerabilities.
  • Determining what to do when a patch or update is not available.
  • Scheduling and executing the remediation activity.
  • Continuous improvement.
• Each remediation option carries a different level of risk that the organization needs to consider and accept by building out this program.
Identify Remediation/Mitigation Options

**Patches and Updates**

Patches are software or pieces of code that are meant to provide fixes to bugs within existing software. These may be provided by the device manufacturer or operating system vendor.

**Configuration Changes**

Configuration changes involve making changes to the device to mitigate the vulnerability. This can include disabling ports and protocols or specific elements and can even extend to removing an application altogether.

**Compensating Controls**

Additional security controls such as firewalls or network access control (NAC), organizations can have as a mitigation mechanism to reduce the likelihood of vulnerabilities beyond the typical patches and configuration changes.

**Risk Acceptance**

When a vulnerability is not remediated the organization is accepting the associated risk.

**Remediation / Mitigation**
Scheduling and Completing

• High and Critical should be completed in a timely manner
• Understand clinical downtime communication and procedures
• Work with clinical staff on scheduling and completing
• Medium to low-risk vulnerabilities can be remediated during PM’s/CM’s
Implementing the Remediation

• Have a rollback plan
• Change control may be necessary
• Understand and document the dependencies
• Is remediation manual or automatic? Evaluate your options for cadence
Phase 4: Post-implementation Activities

Phase 1
- What is vulnerability management?
- Define scope and roles
- Vulnerability detection

Phase 2
- Triage vulnerabilities
- Determine business criticality
- Consider current security posture
- Risk assessment of vulnerabilities

Phase 3
- Assessing remediation options
- Scheduling and completing remediation
- Continuous improvement

Phase 4
- Metrics, KPIs & CSFs
- Vulnerability management policy
- SLA’s
# Metrics, KPI’s and CSFs

- Capture within CMMS/CMDB by creating work orders or tickets

<table>
<thead>
<tr>
<th>Business Goal</th>
<th>Critical Success Factor</th>
<th>Key Performance Indicator</th>
<th>Metric to track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize overall risk exposure</td>
<td>Reduce overall risk due to vulnerabilities</td>
<td>Reduction in the number of vulnerabilities</td>
<td>The number of vulnerabilities year after year.</td>
</tr>
<tr>
<td>Proper allocation of resources</td>
<td>Proper prioritization of mitigation activities</td>
<td>Reduction of critical and high vulnerabilities</td>
<td>The number of critical and high vulnerabilities.</td>
</tr>
<tr>
<td>Consistent &amp; measurable remediation of threats to the organization</td>
<td>Reduce risk when vulnerabilities are detected</td>
<td>Remediate vulnerabilities efficiently within SLA’s</td>
<td>The average time between the identification to remediation.</td>
</tr>
</tbody>
</table>
Tracking Relevant Information

- Not every asset needs a work order for every vulnerability
- KB’s and other documentation should be tracked
- Tracking should take place in all tools (CMMS, active & passive scanning systems)
Key Takeaways

• Invest in IoMT Solution
  • Have a strategy, business case, and integration priority
• Staff to be successful
• Document, track, and record
• Know your devices, environment, and expected outcomes
• Drive policies and procedures along the way and keep refining
Thank You

Please complete the online evaluation/attendance form at https://www.surveymonkey.com/r/ACCE_05-05-22