Medical Device Cybersecurity: Overcoming Challenges to Effective Information Sharing

Session 1, February 19, 2017
Michael C. McNeil, Global Product Security & Services Officer
Royal Philips
Speaker Introduction

Michael C. McNeil, MBA

Global Product Security & Services Officer

Royal Philips
Conflict of Interest

Michael C. McNeil, MBA

Has no real or apparent conflicts of interest to report.
Agenda

• DESCRIPTION:

– This session will present the value propositions for medical device vulnerability information sharing
– Discuss the barriers that continue to create challenges for information sharing.
– Experiences associated with the deployment of a coordinated vulnerability disclosure process
– Highlight the processes for deploying a software medical device bill of materials (SBOM)
Learning Objectives

• Discuss stakeholder value propositions for medical device cybersecurity information sharing

• Illustrate the barriers of implementing cybersecurity sharing

• Explain the rationale and benefits of coordinated disclosure of medical device vulnerabilities

• Describe the rationale and benefits for the sharing of a medical device bill of materials for medical devices
Landscape: The Extended & Connected Ecosystem

**More Connected.**

+ Improved care, more innovation, increased services/efficiency.
- Increased potential of exposure to vulnerabilities and attack.

**Interconnected, Interoperable, and Remote Products/Services.**

- Networks of providers.
- Hospital-to-home.
- Personal health.
- Internet of Things (IoT).
- Remote services.
- Sensitive data storage.
- Sensitive data on-the-move.

**Supply Chain – 3rd Party Suppliers**

- Integrated 3rd party build of materials (BOM).

**Product vs. Component End-of-Life**

- Windows obsolescence.
- Legacy & New
Three Deadly Sins

1. Passwords – fixed, hard coded, default… also shared, easy to guess, posted online, etc...
2. Encryption – at rest, in use, in motion.
3. Patching.

Vulnerabilities To Exploit – Hardware/firmware, network, OS, software BOM, 3rd Party BOMs.

Malware Attacks of Healthcare Facilities ($$↑↑↑), but cheaper and easier.
- Ransomware, Trojans, Remote Command & Control, Data Extraction.
- Via software installs containing malware (installed from a malicious website).
- Via “drive-by downloads” – via website links from a browser on the device.
- Via IM or email attachments – reading the message from the device.

Motivations
- White Hats: Ethical researchers are motivated to improve security.
- Black Hats: Hackers motivated for financial gain, research, social/political, … or just for fun.
Product Security Program Evolution

Governance
- Organizational Alignment
- Executive Leadership visibility (Board, Audit)
- Stakeholder Thought Leadership Strategy (Internal & External) – “Walk the Talk”

Testing
- “Security Ninjas” – dedicated team and Center of Excellence
- Leveraged across the enterprise
- Standardized Use Cases for common and comparable results

Coordinated Vulnerability Disclosure
- Information Sharing (Enhancements and ability to leverage existing Incident Response Management Programs)
- Integrated into Customer Complaint Handling processes

Build of Material
- Continuously monitor software BOM for new vulnerabilities and security SW updates

Maturity Roadmap
- Continuous Assessment and Monitoring of existing modules of the program and seek improvements where appropriate
Common Challenges & Barriers

• Executive Leadership Buy-in

• Competitive Landscape

• Clutter in appropriate venues for developing the culture; sharing and promoting the initiatives; (Trust Factor)

• Where is the win/win for the Ecosystem?
Medical Device Challenges

Could someone walk out with the device?
Could the device be found in an openly accessible area in your facility?

Concerns about anti-virus definition updates on medical devices?
Then is your storage medium encrypted?
Then is the storage medium physically secure so it cannot be removed without tools?

Malware Protection
An application whitelisting solution takes away the need for daily updates.

Can your network and device user be fully trusted to never make an unauthorized connection to the outside world?

Does your device store or display ePHI and could non-authorized users potentially access this?
Is the device only used by clinical users on a daily basis, without a need to access outside of the application?

Firewall Controls
Use a firewall and close all non-essential ports.

How do you share? When do you share? Who to share with (Mfg, HDO, Researchers)????
• 2013-02-22: HTC (mobile phones) settles with FTC by issuing software security patches, and creating a security program to be monitored for 20 years.

• 2013-06-13: FDA and DHS/ICS-CERT require risk information of Medical Device Manufacturers regarding the use of fixed passwords as in over 300 medical devices.

• 2014-03-07: The British Pregnancy Advice Service (BPAS) has been fined £200,000 after a serious breach revealed thousands of records to a malicious hacker.

• 2014-05-07: The Office for Civil Rights (OCR) settles with the New York Presbyterian Hospital and Columbia University for 4.8 million US$ after failing security control led to leak of 6800 patient records onto the internet.

• 2014-08-20: FBI warned US healthcare industry companies that they are targeted by hackers in the new threat where a group of Chinese hackers stole personal information from 4.5 million patients after targeting the computer network of Community Health Systems Inc.

• 2014-11-06: Dutch DPA publishes a report about the Groene Hart Hospital for failing to protect patient information due to the lack of proper network security controls and the ongoing use of end of life software such as Windows 2000 and Windows XP.
Will we see a rise in Cybersecurity Vulnerabilities Communications?
Will we see an increase in coordination of Government Agencies?
Will we see an increase in coordination of Government Agencies?
ICS-CERT Vulnerability Disclosure Policy

• ICS-CERT will attempt to coordinate all reported vulnerabilities with the affected vendor.

• An appropriate timeframe for mitigation development and the type and schedule of disclosure will be determined based on the factors involved. Extenuating circumstances, such as active exploitation, threats of an especially serious nature, or situations that require changes to an established standard may result in earlier or later disclosure.
  – Other factors include:
    • whether the vulnerability has already been publicly disclosed
    • the severity of the vulnerability
    • potential impact to critical infrastructure
    • possible threat to public health and safety
    • immediate mitigations available
    • vendor responsiveness and feasibility for creating an upgrade or patch
    • vendor estimate of time required for customers to obtain, test and apply the patch
The ICS-CERT vulnerability remediation process involves five basic steps:

1. **Detection/Collection**—ICS-CERT collects vulnerability reports in three ways: ICS-CERT vulnerability analysis, monitoring public sources of vulnerability information, and direct notification of vulnerabilities to ICS-CERT. After receiving a report, ICS-CERT does an initial surface analysis to eliminate duplicates and false alarms. ICS-CERT then catalogs the vulnerabilities, including all of the information (public and private) that is known at that point.

2. **Analysis**—Once the vulnerabilities are catalogued, vendor and ICS-CERT analysts work to understand the vulnerabilities by examining and identifying the issues, as well as the potential threat.

3. **Mitigation Coordination**—After analyzing a vulnerability, ICS-CERT will continue to work with the vendor for mitigation and patch issuance. ICS-CERT has established secure and trusted partnerships with control systems vendors for vulnerability disclosure and overall technology assessment and testing functions. ICS-CERT will work with the vendors to allow sufficient time to effectively resolve and perform patch regression testing against any given vulnerability. Additionally, ICS-CERT has experience successfully coordinating response to vulnerabilities that affect multi-vendor products.

4. **Application of Mitigation**—ICS-CERT will work with the vendor to allow sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to disclosure.

5. **Disclosure**—After coordinating with vendors and gathering technical and threat information, ICS-CERT will take appropriate steps to notify end users about the vulnerability. ICS-CERT strives to disclose accurate, neutral, objective information focused on technical remediation and mitigation for asset owners and operators. ICS-CERT will reference other available information and correct misinformation when possible.
How many believe that Information Sharing “Coordinated” Disclosure is a Contact Sport?

Mfg. versus Researcher
Coordinated Vulnerability Disclosure at Philips

(Previously referred to as “Responsible Disclosure”)
Philips Coordinated Vulnerability Disclosure Positioning

• Royal Philips recognizes the need for a clear Coordinated Vulnerability Disclosure Policy and protocols as part of its Product Security function.
• One of the 1st Medical Device company's to implement a Coordinated Vulnerability Disclosure Policy according to current industry best practices. (Post Market Guidance should not enhance and accelerate industry positioning)
  – Our policy is publicly accessible, with clear communications channels for customers, researchers and other security community stakeholders.
  – The policy is based on principles of transparency, accountability and responsiveness.
  – The policy outlines defined protocols for reporting and response, managed by the Philips Product Security Team.
    ▪ The policy protocols encompasses:
      • Monitoring and response of inbound communications
      • Managing confirmation receipt and follow-up communication with senders
      • Evaluation of vulnerability notifications and status tracking
      • Alignment with incident response, stakeholder notification, remediation and prevention protocols as required
• Philips continues to actively seek out researcher and analyst in assistance and guidance towards policy design changes and updates.
  – The company has increasingly engaged with the security research community over the past few years.
  – **Philips is committed to ongoing dialogue with the security community and to productive partnerships.**
Coordinated Vulnerability Disclosure Process
ISO/IEC 29147 and 30111 called out by FDA

Coordinated Vulnerability Disclosure UX00461
(previously referred to as Responsible Disclosure)

Complaint handling / CAPA process should already be in the BU QMS.
For most Healthcare BU’s this is defined by the overarching PHQD in policies such as PHPR0264
Shared responsibilities of the PSSO and the Responsible Organization
Coordinated Vulnerability Disclosure Process Summary

Vulnerability Report Received

• Email Monitoring Team receives email, acknowledges receipt and passes the information to the Event Handler and Responsible Organization.

Verification

• The Responsible Organization initiates the complaint/CAPA process as defined in their local Quality System and verifies the vulnerability.

Resolution Development

• The Responsible Organization executes its standard complaint/CAPA process to determine prioritization and to develop a solution and/or workaround.

Release

• The Responsible Organization releases the solution and/or workaround.

Post Release

• Post mortem analysis by the Responsible Organization shared with the teams.
Why is Coordinated Disclosure (Information Sharing) different?

• For non-customers it is often unclear how or whom to contact within Philips.

• The motivation of the person is often unknown, so the Product Security & Services Office (PSSO) will be the single point of contact. The motivation might be:
  
  – White Hat: An ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of systems (who might be part of a customer organization). Willing to cooperate, no hidden agenda.
  
  – Gray Hat: As above but also personally motivated for compensation either from the organization or by establishing name and fame in the security community (conferences).
  
  – Black Hat: Only out for financial gain. Might be using this process when motivated to damage Philips reputation.
Coordinated Vulnerability Disclosure
is NOT a replacement for Complaint Handling!

The Coordinated Vulnerability Disclosure process precedes the incident response process, adds Product Security & Services Office (PSSO) oversight and inserts additional feedback steps into the standard complaint handling process of the business!
Opportunity to Opening the door for direct communication across the Ecosystem

Since the start of the program in November 2014 we have received 44 reports on vulnerabilities via coordinated vulnerability disclosure:

35 on Philips IT Infrastructure:
- Mainly vulnerabilities on Philips websites

9 on Products:
- 2 Healthcare products
- 2 Personal Health products
- 5 Lighting products (Lights, TVs, Smart Phones)

Currently being deployed globally.

Coordinated Vulnerability Disclosure at Philips (Previously referred to as “Responsible Disclosure”)
Keys to Success

• Better external communication across the ecosystem is critical for a robust security program

• Continuous Threat monitoring of the Healthcare landscape is a critical component in maintaining that vigilance

• Transparency, accountability and responsiveness must be ongoing features, as we maintain and evolve programs

• Wider dialogue between medical device makers, hospitals, regulators and security professionals – particularly around interoperability – will advance innovations in security and the Healthcare industry
Software Bill of Material (SBOM)

• The Cyber Supply Chain Management and Transparency Act of 2014[^8] is pending US legislations that requires government agencies to obtain software BOMs for any new products they purchase. It also requires obtaining software BOMs for "any software, firmware, or product in use by the United States Government."

• Increased customer requirements being written into contracts for governance and disclosure of security vulnerabilities or defects for open source and third party software.
  
  • AAMI’s recent article highlighting Mayo Clinic contract language
  • Veterans Administration (VA) contracts highlighting (NIST 800-53) requirements
  • Department of Defense (DoD) contracts

• Regulatory responsibilities and requirements for the organization to adequately respond to possible security vulnerabilities reported via Accountable Disclosure.
Deploy and integrate the tool on the build servers/code archives on all software products that are developed from Royal Philips.

Scan the software build server/code archive to generate the Bill of Materials.

Inspect the source code and/or binaries of the product.

Correlated with the known security vulnerabilities associated for the components identified.

Security Risk summary report of a product.

• Bill of Materials
• Security Risk Report
Enterprise SBOM Deployment Strategy

Centralized Server and Tools Solution
Available to all Product Lines
Centralized Reporting

Software BOM – Bill of Materials
<table>
<thead>
<tr>
<th>Project name</th>
<th>Version</th>
<th>Vulnerability id</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>commons-logging</td>
<td>1.1.3</td>
<td>CVE-2012-5568</td>
<td>Apache Tomcat through 7.0.x</td>
<td>2.9</td>
</tr>
<tr>
<td>commons-logging</td>
<td>1.1.3</td>
<td>CVE-2013-6357</td>
<td><strong>DISPUTED</strong></td>
<td>6.4</td>
</tr>
<tr>
<td>Apache Commons FileUpload</td>
<td>1.3</td>
<td>CVE-2013-4286</td>
<td>Apache Commons FileUpload</td>
<td>2.9</td>
</tr>
<tr>
<td>commons-logging</td>
<td>1.1.3</td>
<td>CVE-2013-4286</td>
<td>Apache Commons FileUpload</td>
<td>4.9</td>
</tr>
<tr>
<td>commons-logging</td>
<td>1.1.3</td>
<td>CVE-2013-4322</td>
<td>Apache Commons FileUpload</td>
<td>2.9</td>
</tr>
<tr>
<td>commons-logging</td>
<td>1.1.3</td>
<td>CVE-2013-4590</td>
<td>Apache Commons FileUpload</td>
<td>2.9</td>
</tr>
<tr>
<td>Apache Commons FileUpload</td>
<td>1.3</td>
<td>103918</td>
<td>Apache Commons FileUpload</td>
<td>10</td>
</tr>
<tr>
<td>Apache Commons BeanUtils</td>
<td>1.8.3</td>
<td>106409</td>
<td>Commons BeanUtils</td>
<td>6.4</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>v1.1.1</td>
<td>106949</td>
<td>Elasticsearch</td>
<td>6.4</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>v1.1.1</td>
<td>106952</td>
<td>Elasticsearch</td>
<td>2.9</td>
</tr>
<tr>
<td>Spring Framework</td>
<td>4.0.5.RELEASE CVE-2014-3625</td>
<td>Directory traversal</td>
<td>2.9</td>
<td></td>
</tr>
<tr>
<td>Commons IO</td>
<td>2.4</td>
<td>130424</td>
<td>Commons IO</td>
<td>10</td>
</tr>
</tbody>
</table>

Draft Sample Reporting – Illustration Purposes
Bill of Materials Process Summary

- The software BOM will be Integrated into the SDLC process
- Identify software BOM vulnerability's and remediate
- Include software BOM in MDS2 forms and or customer product support documents
- Continuously monitor software BOM for new vulnerabilities and security SW updates
- Update software BOM in MDS2 forms and customer product support documents

BOM – Bill of Material
SDLC – System Development Life Cycle
MDS2 – Manufacturer Disclosure Statement for Medical Device Security (MDS²)
SBOM Success Factors

• Continuous Threat monitoring of the Healthcare landscape is a critical component in maintaining that vigilance

• Transparency, accountability and responsiveness must be ongoing features, as we maintain and evolve programs

• Wider dialogue between medical device makers, hospitals, regulators and security professionals – particularly around software bill of materials – will advance innovations in security and the Healthcare industry
Questions

Speaker

Name: Michael McNeil, MBA
Title: Global Product Security & Services Officer
Organization: Royal Philips
Email: michael.mcneil@philips.com
Phone: 978-659-4571 office.