Market-based public health: collaborative acceleration
Objectives

Define a trusted and repeatable process for medical device manufacturers and HDOs to reduce medical device security vulnerability risks within the operational environment through:

• Increased awareness of security vulnerabilities and impacts
• Improved responsiveness to addressing vulnerabilities within deployed devices
• Mechanisms for information sharing and analytics
Challenges

1. Organization-internal approvals for release of vulnerability information (both HDOs and manufacturers)

2. Creating a secure platform for sharing information

3. Balance of need to limit or anonymize vulnerability data vs. utility of data for analytics

4. Agreement on format and content for information

5. Maintaining process focus on high-impact vulnerabilities

6. Scalability across broad spectrum of vulnerabilities
System Attributes

1. A voluntary market-driven mechanism

2. Process must be consistent with FDA quality system regulation

3. Low risk to Manufacturers and Health Care Providers through application of a common industry process

4. Ensure that access protocols appropriately limit flow of information based; define communication protocols

5. US-based process compatible with global requirements

6. Provide a mechanism to create data for eventual use is a vulnerability analytics system

7. Feedback mechanisms on effectiveness of device vulnerability information
Policy/Guidance Outline

Policy of Medical Device Cyber Security Response Group (MDCSRG) is to promote responsible disclosure of vulnerabilities affecting medical devices via a common collaborative mechanism, open to participation by all stakeholders, within a defined and controlled process, with the goal of mitigating risks to users and patients.
Comments:
Reflect mfg-specific inputs going straight to mfg
Data flows / line for HDOs
Different paths for different level vulns

Users
Public Sources
Researchers

Vulnerability Analysis Team

Manufacturers

Process

General Vulnerability ID
Specific Vuln ID

Assign Vuln Impact Level
Alert to community
Recommend Compensating Controls

ID affected devices
Define Action Plans
Communicate Action Plans
Execute Action Plans

(per defined action process, include safety risk assessment)
(per standard format, at defined time)
Criteria for Input Into Process

- Known engineering event indicating potential for exploit of vulnerability
- Vulnerability affects a widely used software component
- Potential impact to a broad spectrum of deployed medical devices such that the impact would include care delivery impact, patient impact, and/or data protection impact
Patient Safety Domains

Intended Use:

From the FDA Quality System regulation, 21CFR Part 820:

- Manufacturers must maintain procedures to "ensure that the design requirements...address the intended use of the device..."
- Design validation ensures that "devices conform to defined user needs and intended uses."
- "Validation shall ensure that devices conform to defined user needs and intended uses..."
- Risk Management...looks at severity of harm and probability of occurrence...considers failure modes and expected user error...defines a threshold for action

Malicious Use:

Consider potential actions by malicious threat actors
## Ingest Scenarios

<table>
<thead>
<tr>
<th>Reporter</th>
<th>Publicity</th>
<th>Vulnerability Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDA</td>
<td>Private</td>
<td>General-Purpose</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device-Specific</td>
</tr>
<tr>
<td></td>
<td>Public</td>
<td>General-Purpose</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device-Specific</td>
</tr>
<tr>
<td>ICS-CERT</td>
<td>Private / Public</td>
<td>General / Specific</td>
</tr>
<tr>
<td>Individual Researcher</td>
<td>Private / Public</td>
<td>General / Specific</td>
</tr>
<tr>
<td>Public Feeds (e.g. CVE/NVD)</td>
<td>Private / Public</td>
<td>General / Specific</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

“0-day” (public without a patch) is an important consideration, as is active exploitation.
Triage Decision Logic

Vulnerability discovered

- Vulnerability specific to Med Device
  - Yes: Triage for Advisory
  - No
    - Vulnerability has gained widespread attention
      - Yes: Triage for Advisory
      - No
        - Vulnerability affects general computing platform
          - Yes: Triage for Advisory
          - No
            - Platform known to be used in a Med Device
              - Yes
                - Platform known to support clinical software supporting a Med Device
                  - Yes: Triage for Advisory
                  - No
                    - Can data call requesting additional data from manufacturer be initiated
                      - Yes: Triage for Advisory
                      - No
                        - Add block for safety assessment
                          - Yes
                            - No action
                            - Triage for Advisory
                          - No
                            - Triage for Advisory
            - No
              - Platform known to be used in a Med Device
                - Yes: Triage for Advisory
                - No
                  - Add block for safety assessment
                    - Yes
                      - No action
                      - Triage for Advisory
                    - No
                      - Triage for Advisory

This is the "specific" case

This is the "general" case
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Mfg provides content for post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public domain vuln, comes to attention of NH-ISAC</td>
<td></td>
</tr>
</tbody>
</table>

(this chart not complete)
### Example: Vulnerability Impact Levels

#### Potential impact assessed at Triage level:

<table>
<thead>
<tr>
<th>Impact Value</th>
<th>VIL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>Level 3</td>
<td>This vulnerability could be expected to allow a threat event with multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.</td>
</tr>
<tr>
<td>High</td>
<td>Level 3</td>
<td>This vulnerability could be expected to allow a threat event with a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Level 2</td>
<td>This vulnerability could be expected to allow a threat event with a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.</td>
</tr>
<tr>
<td>Low</td>
<td>Level 1</td>
<td>This vulnerability could be expected to allow a threat event with a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.</td>
</tr>
<tr>
<td>Very Low</td>
<td>Level 1</td>
<td>This vulnerability could be expected to allow a threat event with a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.</td>
</tr>
</tbody>
</table>

**Actual impact must be assessed at device level**
## Example: Vulnerability Impact Levels

<table>
<thead>
<tr>
<th></th>
<th>Negligible</th>
<th>Limited</th>
<th>Serious</th>
<th>Severe</th>
<th>Multiple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Assets</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Individuals</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Nation</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Mission Capability</td>
<td>N/A</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Minor Asset Damage</td>
<td>N/A</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Minor Financial Loss</td>
<td>N/A</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Individual Harm</td>
<td>N/A</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Life-threatening or Loss</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>High</td>
<td>Very High</td>
</tr>
</tbody>
</table>
## Response Process for Vulnerability Impact Levels

<table>
<thead>
<tr>
<th>Level 3</th>
<th>Actions</th>
</tr>
</thead>
</table>
| 1) Vulnerability Alert sent to manufacturers; vulnerability alert posted  
2) Manufacturers perform safety risk assessment consistent with 21CFR Part 820 requirements  
3) Manufacturers initiate appropriate corrective action process for safety risks |
| If no safety-related action, address non-safety risks:  
4) Manufacturers perform non-safety risk assessment (malicious activity risk, privacy risk)  
5) Manufacturers define action plans to address non-safety risks  
6) Manufacturers document product info and action plans per standard format for affected products  
7) Info within Comm Portal data made available to authorized subscribers (per defined timing) |

| Level 2 | Same as Level 3, except:  
Manufacturers input info into Comm Portal ONLY if a product action is planned |

| Level 1 | 1) Vulnerability Info posted in Comm Portal; defines as Level 1 “low impact”  
2) Manufacturers determine need for further action |
Vulnerability Communication Data

Data provided by manufacturer per product affected:
Vulnerability / CVE # (as applicable)
Manufacturer
Product Name / Identifier
Vulnerability Impact Description
Safety Impact per 21CFR (yes/no)
Action Plan (description of planned action and timing)
Rationale for Defined Action
Contact information
Pilot / Implementation Assessment

**Front End**
- Industry Group Review and Impact Assessment of Vulnerability + Alert
  - Easier to pilot

**Back End**
- Manufacturer Communication / Action
  - Harder to pilot

**Process**
- Manufacturer Product Review and Action Plan Process
Demo Scenario
Implementation Concerns

Perceived risk from inter-relationship with safety management process, however process is designed to avoid this risk

Need to clearly delineate process and flows within and outside the Quality Regulation
NextBleed - Scenario

- Security researcher announces discover of a vulnerability affecting Unix-based systems, with potential wide impact across multiple types of products. This vulnerability would allow an unauthorized user to gain access…

- Press release and related information is reviewed by several key medical device manufacturers, MITRE, etc.

- Multiple manufactures notify the secretary of the Medical Device Cyber Security Response Group (MDCSRG), to include this vuln on the agenda of the next Vulnerability Response Team (VRT) meeting

- VRT meets and designates the vulnerability as a “level 3”

- VRT prepares an alert statement for the subscriber community
Vulnerability Response Team

Representation from:
- Manufacturers
- MITRE
- Health Delivery Orgs
- Security Industry
- Researcher community
- Observance from FDA

Total group 10-12?

Roles: Chairman, Vice Chairman, Secretary
New Vulnerability Alert: NextBleed

Vulnerability Alert: NextBleed 20 February 2015

A security vulnerability has been identified that may impact a large number of medical devices that utilize a Unix variant or run Unix-variant services on Windows. This vulnerability has been assessed as a Level 3 vulnerability by MDCSRG. It is exploitable over network connections by various methods and the exploit does not require authentication.

MDCSRG has initiated response actions by all member manufacturers. This response includes identification of affected products, assessment for patient safety risk per the regulated safety risk management process, and assessment for non-safety actions to mitigate data protection and other malicious activity risks. Manufacturers are requested to provide product information and action plans to subscribing customers 30 days following this alert – 20 March 2015.

For a list of participating manufacturers, CLICK HERE

Overview:

The NextBleed vulnerability is a vulnerability that affects all systems running the Bash login shell on variants of Unix (e.g. Linux, MacOS, HELiOS, Sun Solaris etc.). The Bash shell is the default shell for a majority of Unix-based systems produced in the past 25 years and the vulnerability is present in all versions of Bash released through today. Numerous media outlets are reporting that exploits have been seen in the wild and that the penetration testing tool Metasploit has added a module to exploit the vulnerability on affected systems.
Response Process by Manufacturer

1) Manufacturer A identifies products in service affected by vulnerability

2) Manufacturer A performs safety risk assessment on affected products consistent with 21CFR Part 820 requirements

3) Manufacturer A does not identify any products with patient safety risk such that the risk level requires action within the safety recall process

4) Manufacturer A performs non-safety risk assessment (malicious activity risk, privacy risk) on affected products

5) Manufacturer A defines action plans to address non-safety risks

6) Manufacturer A documents affected products and action plans per standard format for affected products

7) Info is distributed to authorized subscribers

NOTE: Complete within 30 days
<table>
<thead>
<tr>
<th>Vulnerability Name</th>
<th>Product Type</th>
<th>Products Affected</th>
<th>Patient Safety Impact</th>
<th>Action Description</th>
<th>Action Target Date</th>
<th>Comments/Rationale</th>
<th>ACTION STATUS</th>
<th>Contact</th>
</tr>
</thead>
</table>
| Shellshock        | Image Archive | Product Alpha 1.0  | No                    | Software update in development | 11/20/2014        | The communication outlined installation of the two patches from Microsoft at the client sites after testing on the product by Engineering. Two technical bulletins were constructed and communicated via ITPS and distributors. | DONE          | John Smith  
john.smith@ge.com  
262-555-1234 |
| Shellshock        | Surgical XR  | Product 1000      | No                    | Product update not required, will provide additional info for customers | 12/11/2014        | Investigation Summary:  
While several products in the Surgery portfolio use versions of bash that are vulnerable, there is no increased safety risk to patients. Compliant analysis did not indicate that any code was run remotely and there was no evidence of system parameters being changed. Additionally there is no evidence that local and remote system passwords were compromised. These systems do not use any web services or use bash as an interpreter for Common Gateway Interface (CGI) scripts so that attack vector is inconsequential. The systems do allow limited remote access using Secure Shell (SSH) for serviceability but only through authenticated connections with private passwords and usernames. Locally, to use bash, the systems need to be booted into a service menu and user authenticated as well, this would require physical system access, therefore the Shellshock CVE-2014-7169 vulnerability presents no safety risk to patients. | IN PROCESS    | John Smith  
john.smith@ge.com  
262-555-1234 |
Incident Data

As a follow-up step we may create a data flow to address collection of incident data that relates to medical device vulnerabilities.

This data would flow from the HDOs, and would be useful to other HDOs and manufacturers to help determine risk level of a vulnerability.
Vulnerability Sharing – Pilot Objectives

Establish a pilot process:

• Identify a set of known vulnerabilities for impact review (manageable number - represent a spectrum)

• Identify participants for Pilot vulnerability analysis team

• Identify impact level for sample vulnerabilities

• Draft sample “alert statements” to send to Mfgs / HDOs

• Manufacturers response plans - affected w/action, affected w/no action, not affected, timing, etc.

• Manufacturer communication naming conventions – mapping info to assets

• Manufacturer assessment of industry-level response process and mechanisms

Pilot evaluation / working process documentation

Education / Communication / Implementation Plan
Comments

• Would group have ability to react quickly to vulns – can it be effective operationally, need operational mechanisms responsive to urgent needs

• Need a comm work flow with info from various stakeholders (both within healthcare and outside experts)

• How can we link product inventories to pertinent data – standardized numbering systems, etc.

• Leverage any existing systems, NH-ISAC or other, as much as possible

• Would sharing network potentially violate NDAs – need to rework NDAs?

• (ideally flow goes first through mfg, then into sharing network)

• Define time tables
Process Document Outline

1. Purpose and Scope

2. Roles and Responsibilities
   • Manufacturers
   • HDOs
   • NH ISAC
   • Collaborative Researchers
   • FDA / DHS
   • Others?

3. Process Flow / Steps
Purpose and Scope

Purpose:
Provide a mechanism to reduce cyber security-related risks within the healthcare environment through collaborative information sharing among device manufacturers, Health Care Providers, Security Researchers, and Government partners. Participation in this mechanism will be voluntary.

Scope:
This process will be applicable to medical devices used in US (initial scope), with potential for expansion to other devices pertinent to healthcare-specific IT.
Roles and Responsibilities

Medical Device Vulnerability Response Board (MD-VRB)
• Provide membership opportunity to manufacturers, HDOs, cyber security experts, …
• Review incoming information and determine response level
• Determine appropriate timing for release of information
• Define or Review common mitigation recommendations and urgency level

NH-ISAC
• Provide a mechanism for disclosure of vuln info to member orgs

Medical Device / Healthcare IT Device Manufacturers
• Review sources of information for identification of cyber vulnerabilities
• Identify vulnerabilities / potential vulnerabilities
• Report potential vulnerabilities to Medical Device Vulnerability Response Board (MD-VRB)
• Determine product applicability
• Perform risk analysis to address patient safety risk within intended use
• Perform risk analysis and needed actions to address cyber risks
• Recommend short term action for affected products
• Initiate design change actions as appropriate
• Input applicable info pertaining to vulns, affected products, and actions to communication mechanism
Health Delivery Organizations

- ID Vulnerabilities
- Comm to mfg through appropriate mechanism
- Assessment of exposure level for a given vulnerability
- Maintain up to date documentation on network architecture to support vuln risk assessment

Vulnerability Analysis Team

- Assess appropriate response level for vulnerabilities affecting medical devices
- Provide direction to manufacturers to follow appropriate response process for the determined risk level of the vulnerability
- Ensure responses are completes as appropriate for vuln levels
- Provide guidance to stakeholders on response requirements and content
Vulnerability Management System

System Design
• Work flows / data flow schematic
• Functional requirements
• Business requirements
• Operational characteristics for system

Implementation requirements / obstacles

Project Plan and Milestones

Performance Measures