Joint Security and Privacy Committee

NEMA COCIR JIRA

International Medical Informatics

Patching Off-the-Shelf Software

Used in Medical Information Systems

This Paper was developed by the
Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)

This Paper has been approved by:
NEMA (National Electrical Manufacturers Association-USA)
COCIR (European Coordination Committee of the Radiological and Electromedical Industry)
JIRA (Japan Industries Association of Radiological Systems)

October 2004

Endorsed by:
AdvaMed (Advanced Medical Technology Association)
ACCE (American College of Clinical Engineering)

Reviewed and Approved by:
Privacy & Security Steering Committee of HIMSS
(Healthcare Information and Management Systems Society)

Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org/medical
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA tel: 703-841-3200 fax: 703-841-5900
Secretary: Stephen Vastagh, tel: 703-841-3281; fax: 703-841-3381 E-mail ste_vastagh@nema.org

1. Purpose and Scope

Medical Information Systems (MedIS[1]) often incorporate commercial-off-the-shelf (COTS) software, e.g. operating systems, browsers, databases. COTS software vendors often issue patches, also called “hotfixes” or “updates,” to fix a variety of security, privacy, or stability problems. Typically, COTS software vendors’ procedures for testing or updating do not address the safety and effectiveness requirements mandated for MedIS. This means that healthcare providers must follow different procedures when patching COTS software incorporated in MedIS.

The purpose of this white paper is to make healthcare providers aware of the special requirements imposed on MedIS vendors and the practical constraints involved in patching COTS software.

Updates of the medical application software itself, as opposed to the underlying COTS software, are outside the scope of this White Paper. These changes will be processed in accordance with the configuration management procedures required by the quality system used by the MedIS vendor. Similarly, updates that simply add functionality rather than address vulnerabilities are not addressed here.

Network security is a shared responsibility that requires both the vendors and the users of MedIS to contribute to the solution. Patches are just one piece of a proper Defense In Depth strategy. A broader discussion of defenses against malicious software (malware) attacks can be found in the SPC white paper “Defending Medical Information Systems Against Malicious Software.”[2]

2. Introduction

The globally increasing threat to IT systems in general, is due in part to malicious software exploiting vulnerabilities. This affects MedIS vendors and healthcare providers alike. Exploitation of the most severe of such vulnerabilities would allow a malicious user to take control of a MedIS, make it unavailable, or corrupt the data it works with.

Combating malware and addressing emerging IT vulnerabilities can require obtaining and installing periodic updates to the software components of such systems. In the office environment, healthcare providers frequently obtain and install such updates themselves. In contrast, the deployment of patches on MedIS must meet special requirements, which include the following:

- The MedIS vendor and the healthcare provider are required, by law or contract to assure continued safe and effective clinical functionality of their products.
- Adequate testing must be done to discover any unanticipated side effects of the patch on the MedIS (performance or functionality) that might endanger a patient.

[1] MedIS generally includes all information systems directly employed in delivering health care. Examples include, but are not limited to: HIS (Hospital Information System), PACS (Picture Archiving and Communication Systems), imaging modalities, radiation therapy systems, and patient monitoring systems.

[2] The full text is available at http://www.nema.org/medical/spc.

Due to these requirements, updates to MedIS should involve the MedIS vendor. The necessary procedures to be defined by the MedIS vendor and to be adhered to by healthcare providers are explained below.

3. Patch Deployment: Needs and Constraints

This section outlines the typical stages of the process to deploy a patch on a MedIS and describes, for each stage, the needs of the parties involved and the constraints that exist as to how the stage may be conducted.

3.1 Availability Awareness

The update process is triggered by the release of a patch from a COTS software vendor that removes a newly discovered vulnerability. Vendors and users need to be aware of new vulnerabilities in a timely fashion since some may warrant prompt action. MedIS vendors will monitor the release of patches for COTS software that their products use. Users should also monitor patch releases since many of the risks apply across their IT infrastructure. Due to the number of patch releases and the low percentage that impact safety, it is impractical for vendors to notify users at the release stage.

3.2 Vulnerability Risk Assessment

Once the patch is announced, it is necessary to understand the potential risk posed by the vulnerability addressed by the patch. MedIS vendors will first evaluate the impact of the vulnerability on the further proper and safe operation of this system. The evaluation will consider both the likelihood that the vulnerability will be exploited and the impact to the MedIS and other systems if exploited. The Common Vulnerabilities and Exposures[3] classification system may be used as shared vocabulary and for assessing the severity of a vulnerability.

The actual threat may vary for each MedIS product or product category depending on how the COTS software is used. Many mitigating factors can reduce or even eliminate the potential security consequences of a vulnerability. For vulnerabilities that affect a component that is disabled or not installed in the MedIS, or vulnerabilities that otherwise pose minimal risk to the system, the MedIS vendor may properly decide not to release the patch.

3.3 Patch Impact Analysis

It is also necessary to understand the potential impact that the patch itself may have on the MedIS. Installation of patches typically influences the behavior or interfaces of several COTS components, which in turn interact with other MedIS software. Analysis to identify and evaluate these interactions can be complex and may require significant time and effort for the MedIS vendor to complete. It is even conceivable that the impact of the patch may be worse than the impact of the vulnerability. The vendor will also consider the possible effects of a failed update.

[3] http://cve.mitre.org

For patches that the vendor decides warrant release, this analysis will guide the validation strategy and determine which functionalities will need to be tested.

For patches that present unacceptable risks, the MedIS vendor needs to define and implement risk mitigation measures. The remaining risk must be in an acceptable range.

3.4 Patch Validation

MedIS vendors need to assure proper functionality of their properly maintained products. It is important for healthcare providers to realize that before such patches are installed, they must to be validated by the MedIS vendor. MedIS vendors are ultimately responsible for the approval of patches they provide.

The formal validation process, which has to meet relevant regulations (e.g. FDA if the MedIS is a medical device marketed in the United States), at a minimum must ensure the following:

- The patched MedIS continues to work as intended.
- The patch meets the specifications as described by the COTS software vendor.
- The patch does not compromise the safety and effectiveness of the MedIS.
- The patched MedIS still meets legal requirements.
- The patched MedIS remains maintainable.
- The patch itself is free of malware.

The validation process can require considerable time and effort on the part of the MedIS vendor.

3.5 Patch Delivery

The validated patch needs to be delivered to each system on which it will be installed. The patch delivery process itself needs to be defined and validated to ensure that the patch as validated and released by the MedIS vendor is delivered to the specific MedIS. Some basic requirements are:

- The delivery must maintain the integrity of the patch. Possible measures vary depending on the delivery medium employed, e.g. a physical medium (CD-ROM or floppy disk) or a data network to transfer the software update as a file.
- A clear indication may be given to the person performing the delivery of successful or unsuccessful delivery.

Vendors face practical constraints that may impact the speed and frequency with which patches are delivered.

3.6 Patch Installation

Validated and delivered patches need to be installed on each MedIS. Some minimum requirements on the installation process are:

- The healthcare enterprise and the vendor must ensure the installation process does not interfere with clinical use of the MedIS. For example, automated updates, if used, must be scheduled to occur only at times when the MedIS is not being used for patient care.

- A clear indication must be given to the person performing the installation of successful or unsuccessful completion of the process.
- If the installation was unsuccessful, the MedIS must fall back to a safe and validated operating condition.
- The installation procedure should include a method for confirming the newly updated device is performing as expected following installation.

The MedIS vendor will evaluate the best practice for installation based on service staff availability, the nature of the impact of the system patch and the complexity of actions required to complete the installation process. This best practice will include involvement with the healthcare provider to assure there is staff availability, minimal impact to patient scheduling and equipment availability resulting in an optimal installation process. For example, the installation may require on-site support, may be performed over a remote servicing connection, or perhaps involve the user staff. The MedIS vendor decision for optimal installation may be that the patch deployment be individually scheduled, performed on a regular cycle, or included in a system upgrade.

4. Conclusion

Users may learn of patches to COTS software used by their MedIS through the news media or other public source. Accustomed to rapid patches of general-purpose computers, they may be frustrated when MedIS vendors do not provide equally rapid patches to MedIS. However, they must recognize that the MedIS vendor has additional responsibilities to meet medical safety and effectiveness concerns. Not all security, privacy, and stability patches from COTS software raise the safety and effectiveness concerns that warrant the cost and effort involved in deploying the patch.

MedIS vendors determine the relevance of a patch through a risk assessment. Our goal is to reassure users that MedIS vendors take their obligations seriously to maintain the safe operation of their systems and provide the quality required for patient care. Meeting those obligations requires that patches go through the somewhat time-consuming process described above. MedIS vendors do recognize the need to release relevant and safe patches in a timely fashion.

Equally important is that the users must take vital steps to protect patient safety while this process runs its course by securing their networks and protecting their MedIS. The users need to develop a risk assessment strategy that builds on: status of active threats, MedIS patch availability, defense in depth strategy, business continuity planning, etc.

Bypassing the risk assessment and validation steps may seem appropriate in the face of a malware attack that requires fast response. However, doing so jeopardizes the mission shared by MedIS vendors and healthcare providers to proper delivery of healthcare.

=====================================