FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks

U.S. Food & Drug Administration

Date Issued: June 13, 2013

Audience: Medical device manufacturers, hospitals, medical device user facilities, health care IT and procurements staff; and biomedical engineers

Issue: Cybersecurity for medical devices and hospital networks

Purpose: The FDA is recommending that medical device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks.

Summary of Problem and Scope: Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches. In addition, as medical devices are increasingly interconnected, via the Internet, hospital networks, other medical device, and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates.

Recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including:

- Network-connected/configured medical devices infected or disabled by malware;
- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices);
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection.

The FDA is not aware of any patient injuries or deaths associated with these incidents nor do we have any indication that any specific devices or systems in

clinical use have been purposely targeted at this time.

The FDA has been working closely with other federal agencies and manufacturers to identify, communicate and mitigate vulnerabilities and incidents as they are identified.

Recommendations/Actions:

Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches.

For all device manufacturers:

Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity, and are responsible for putting appropriate mitigations in place to address patient safety and assure proper device performance.

The FDA expects medical device manufacturers to take appropriate steps to limit the opportunities for unauthorized access to medical devices. Specifically, we recommend that manufacturers review their cybersecurity practices and policies to assure that appropriate safeguards are in place to prevent unauthorized access or modification to their medical devices or compromise of the security of the hospital network that may be connected to the device.Â The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach.

In evaluating your device, consider the following:

- Take steps to limit unauthorized device access to trusted users only, particularly for those devices that are life-sustaining or could be directly connected to hospital networks.
  Appropriate security controls may include: user authentication, for example, user ID and password, smartcard or biometric; strengthening password protection by avoiding hard-coded passwords and limiting public access to passwords used for technical device access; physical locks; card readers; and guards.
- Protect individual components from exploitation and develop strategies for active security protection appropriate for the device’s use environment. Such strategies should include timely deployment of routine, validated security patches and methods to restrict software or firmware updates to authenticated code. *Note: The FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity.*
- Use design approaches that maintain a device’s critical functionality, even when security has been compromised, known as “fail-safe modes.”
- Provide methods for retention and recovery after an incident where security

has been compromised.
Cybersecurity incidents are increasingly likely and manufacturers should consider incident response plans that address the possibility of degraded operation and efficient restoration and recovery.

For health care facilities:

The FDA is recommending that you take steps to evaluate your network security and protect your hospital system. In evaluating network security, hospitals and health care facilities should consider:

- Restricting unauthorized access to the network and networked medical devices.
- Making certain appropriate antivirus software and firewalls are up-to-date.
- Monitoring network activity for unauthorized use.
- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.
- Contacting the specific device manufacturer if you think you may have a cybersecurity problem related to a medical device. If you are unable to determine the manufacturer or cannot contact the manufacturer, the FDA and DHS ICS-CERT may be able to assist in vulnerability reporting and resolution.
- Developing and evaluating strategies to maintain critical functionality during adverse conditions.

FDA Activities:

The FDA has been working closely with other federal agencies and manufacturers to identify, Â Â communicate and mitigate specific cybersecurity vulnerabilities.

The FDA released a draft guidance on how manufacturers should address cybersecurity in their pre-market submissions. The FDA also has guidance on how manufacturers should address cybersecurity issues related to products that use off-the-shelf software.

Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with medical devices. If you suspect that a cybersecurity event has impacted the performance of a medical device or has impacted a hospital network system, we encourage you to file a voluntary report through MedWatch, the FDA Safety Information and Adverse Event Reporting program.

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Device manufacturers must comply with the Medical Device Reporting (MDR) regulations.

To help us learn as much as possible about any cybersecurity issue with a specific medical device, please include the following information in your reports, if available:

- Who is the point of contact for providing more information about the event?
- When and how was the information security/cybersecurity issue first discovered?
- What specific model numbers and firmware versions are affected?
- How many devices are affected?
- Has the device functionality been compromised? If so, how was the vulnerability exploited (for example, was it exploited remotely or via local access)?
- What is the observed abnormal behavior of the device?Â What are the possible consequences?

Contact Information:

If you have questions about this communication, please contact the Division of Small Manufacturers, International and Consumer Assistance (DSMICA) at DSMICA@FDA.HHS.GOV [1], 800-638-2041 or 301-796-7100.

To assist in reporting a specific medical device vulnerability, contact ICS-CERT at 877-776-7585 or ics-cert@dhs.gov [2].

Recommended Readings

1. NIST Special Publication 800-82, Revision 1, May 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf [3]
2. DHS-ICS-CERT “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” October 2009 http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf [4]
3. ICS-CERT Web Site, http://ics-cert.us-cert.gov/ [5]

Source URL (retrieved on *04/18/2015 - 1:33pm*):
http://www.mdtmag.com/news/2013/06/fda-safety-communication-cybersecurity-medical-devices-and-hospital-networks?qt-most_popular=0&qt-video_of_the_day=0

Links:
[1] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/mailto:DSMICA@FDA.HHS.GOV
[2] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/mailto:ics-

cert@dhs.gov
[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf
[4] http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf
[5] http://ics-cert.us-cert.gov/