MEDIGATE

Medical Device Patching In Clinical Networks: **Why It Is Not Enough**

Why Patching Is Not Enough

Years of experience in cybersecurity show that timely patching of security flaws in network-facing software is a critical component of any mitigation effort. Indeed, regular acquisition and application of security patches are part of the toolkit of any modern cyber security team. One would not expect deviation from this practice in the increasingly connectivity-oriented field of medical devices. However, it turns out that what works for a personal computer or web server is not necessarily applicable to a legacy, FDA approved life-saving medical device. The vast increase in cyber attacks on the healthcare industry in recent years is evidence enough that we should rethink our defensive strategies. If you're a cyber security official in the healthcare industry, this paper could be of value for you.

Medical Device Vulnerabilities

Medical devices, like IT and IoT systems, are vulnerable to security breaches that may potentially impact their safety. The degree of vulnerability grows as medical devices become increasingly connected to hospital networks and to other medical devices, thus expanding the attack surface and introducing new attack vectors that could be exploited by cyber criminals. These vulnerabilities are indeed being exploited as seen in recent incidents. However, it is difficult to estimate the precise magnitude of medical device attacks since incidents aren't always reported.

Generally, with medical devices, a software vulnerability is a security weakness found either in an operating system or software application running on the device. Hackers exploit this weakness by writing code targeting a specific vulnerability, which is packaged into malware. Medical devices can run on proprietary or COTS (commercial off-the-shelf) Operating Systems. In medical networks, both OS and the manufacturers' coded applications are vulnerable. This raises the question: which software is more susceptible to cyber-attacks? The answer is not entirely clear. On the one hand, medical devices using COTS OS are exposed to numerous cross-sector vulnerabilities that may affect them even in the case of an untargeted attack. On the other hand, medical devices use designated application layer protocols such as DICOM and HL7, exposing the devices to application specific attacks, which are not addressed by today's cybersecurity solutions.

The Manufacturers' Perspective - Medical Device Patching Process

Research

Testing

Validation

Verification

Documentation

Notification

Distribution

According to IBM 2017 X-Force Threat Intelligence, healthcare is now the most attacked industry. Moreover, according to HIMSS 2016 State of the Market report, showed that during 2015 there was a significant increase relative to previous years in the number of health providers that have been hacked, and the impact on patients as a result.

> **An attack doesn't have to target medical devices in order to damage these kinds of systems. In fact, many medical devices run on COTS OS, which enable untargeted attacks using common COTS vulnerabilities to access clinical networks and harm medical devices.**

An attack doesn't have to target medical devices in order to damage these kinds of systems. In fact, many medical devices run on COTS OS, which enable untargeted attacks using common COTS vulnerabilities to access clinical networks and harm medical devices.

In many cases, cyber criminals will utilize all available attack vectors without knowing the identity of their target, in hope of exploiting an unpatched vulnerability.

FDA Directive

To address this concern, the FDA issued an update last year to their policies as part of its goal to help bolster the security of medical devices.

Normally, medical device manufacturers must comply with FDA federal regulations. As part of these regulations, manufacturers must submit a mandatory application to the FDA during the pre-market process and update regarding any changes during the post-market process, if those changes will affect the intended use of a device or introduce any new elements of risk. According to the new policies, medical device manufacturers can almost always update a medical device when it comes to cybersecurity, and the FDA does not typically need to review changes made to medical devices solely for strengthening cybersecurity. While this doesn't necessarily represent a major change in approach (this had been a part of previous policy), it clarifies the FDA's attitude towards medical device security and emphasizes the importance of protecting these devices.

Suzanne B. Schwartz, FDA's Associate Director for Science and Strategic Partnerships at the Center for Devices and Radiological Health:
"It is the goal of FDA to encourage a coordinated approach of vigilance, responsiveness, resilience, and recovery that fits our culture of continuous quality improvement. This means taking a total product lifecycle approach. Specifically, FDA encourages medical device manufacturers to proactively update and patch devices in a safe and timely manner."

This change is welcome and will drastically reduce the time it takes to issue a patch after a medical device vulnerability has been identified.

The inevitable question that arises is: is this enough? Will the patching processes of security vulnerabilities in medical devices be timely enough to mitigate all imminent threats? Probably not. Unlike traditional information technologies, mission critical systems are much more complicated and require a collaborative approach, as we will describe below.
There are two main stakeholders involved in the process of patching medical devices, the HDO (Healthcare Delivery Organization) and the manufacturers.

The Manufacturers' Perspective

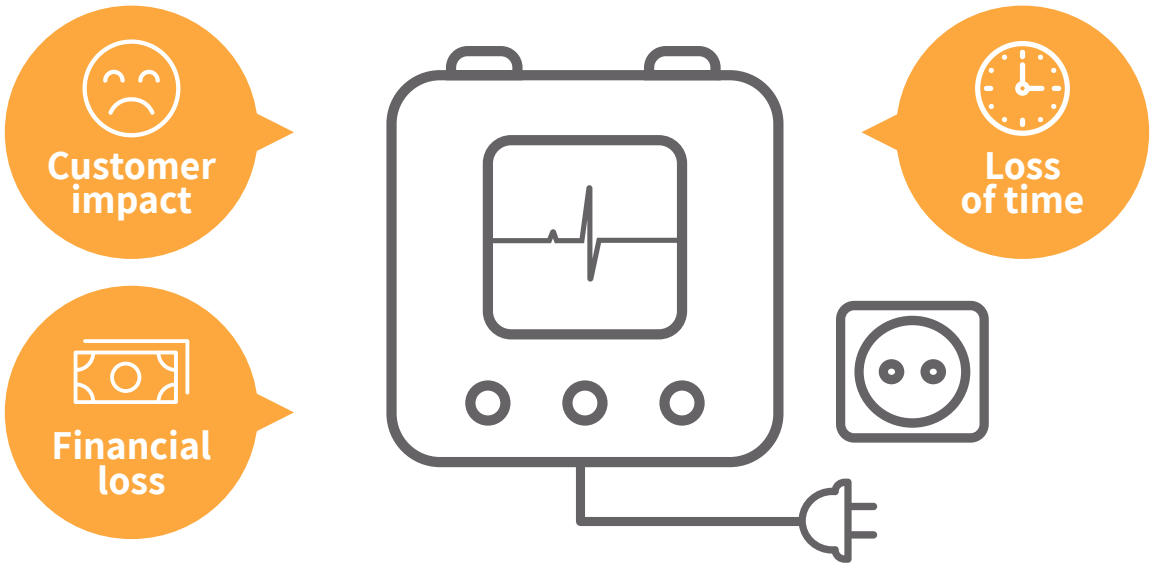
According to FDA policy, medical device manufacturers are responsible for the validation of all software design changes, including those that address cybersecurity vulnerabilities. Because of this, manufacturers must strictly and independently manage their examination and quality process. This process follows similar steps to the formal FDA regulation process, meaning it is somewhat complex and requires time and effort. It begins with testing, verification and validation, followed by documentation, customer notification, and distribution. The duration and timing of this workflow are dependent on a manufacturer's quality systems, and the entire procedure often extends over a long period of time due to the lengthy examination process and the extra care taken to ensure the uncompromising quality of the medical devices.

> **Making matters more complex, unlike traditional IT systems, it is common for medical devices to be used over a long life cycle. This longevity creates a situation where medical devices using COTS operating systems run on unsupported versions that are no longer updated with vendor security patches.**

Making matters more complex, unlike traditional IT systems, it is common for medical devices to be used over a long life cycle. This longevity creates a situation where medical devices using COTS operating systems run on unsupported versions that are no longer updated with vendor security patches.

Even in cases where security patches are being released frequently; consequently, many medical device manufacturers are challenged to test and validate them in order to provide timely releases. For example, Microsoft usually releases updates for the various Windows operating systems around once a month. These updates cannot be immediately applied to medical devices in their original structure, but need to go through the manufacturer's quality testing process and be adapted to the specific embedded device by the manufacturer. In the case of the WannaCry attack, hackers exploited a previously known vulnerability that affected various Windows operating systems, including Windows XP, which had been previously patched by Microsoft before the attack, but many manufacturers had yet to incorporate this patch at the time. In that case, although Microsoft no longer supported the XP version, they chose to publish a patch anyway, since the vulnerability was deemed to be critical. However, due to the dynamics outlined above, many manufacturers had yet to incorporate this patch at the time.

The HDO's Perspective - The Difficulties in Medical Device Patching



The HDO's Perspective

While unplugging or rebooting a personal computer is usually not a problem, and even web applications can be brought down for scheduled maintenance while a backup is running, medical device updates require that the device be turned off. This requirement results in disrupted hospital activities when a device is being updated.

> **Many devices have around the clock 24/7 operational requirements and any interruption can have serious operational and safety implications. HDO must strike a delicate balance when considering optimizing patients welfare and managing cyber threats.**

Many devices have around the clock 24/7 operational requirements and any interruption can have serious operational and safety implications. HDO must strike a delicate balance when considering optimizing patients welfare and managing cyber threats.

Furthermore, medical networks are much more complex than standard IT networksas they generally contain a thousands of unique, highly specialized devices. In many cases, given the complexity and diversity of the medical devices, HDO IT teams find it difficult to manage efficient patching practices. Compounding the complexity of the environment even more, in some cases there is ambiguity around ownership of the patching process within an HDO due to organizational divisions between healthcare IT and biomed engineering teams, both of which are required for patch distribution and installation. Taken together, these issues typically cause practical difficulties and disincentivize organizations from pursing necessary updates.

Lack of Communication between the HDO and the Manufacturers

Frequently, there is no defined work flow between the HDO and the manufacturer for distributing and communicating patches. Moreover , there are in fact contradictory interests between the two. On the one hand, the HDO normally doesn't have the detailed knowledge required to drive decisions about necessary patches and therefore has little influence on the process. Even when it comes to issues with COTS operating systems, an HDO won't have good visibility into its vulnerabilities or into which patches are relevant for them, as they generally lack familiarity with the OS versions in question. On the other hand, for the manufacturers, security is not always a top priority. Manufacturers usually prefer to focus on functionality issues and improve their users' satisfaction. In addition, the fact that medical devices are typically not supposed to be connected to the Internet, further complicates the process, requiring it to be done manually by a field engineer or by remote access in some cases.

Thus far, we have focused on what happens after a security vulnerability is identified, but who is responsible for finding these vulnerabilities in the first place? Unlike traditional systems, where there is a large group of researchers looking for security weaknesses, finding a medical device weakness is almost completely dependent on the manufacturers. Getting access to medical devices is hard. Not only are these products expensive, but one must own a license in order to purchase them. Furthermore, while most systems' firmware is public, making it easy for anyone with an Internet connection to research, medical device manufacturers do not publicly publish their products' firmware. This policy, known as "security by obscurity," relies on the secrecy of the design or implementation as the main security method for a system or system component. This approach is problematic. Not only is there no access to outside help and analysis from experts all over the world who could provide value to manufacturers and their systems, but this also provides a false sense of security. The manufacturers believe that they are "completely covered" and security is no longer at the forefront as one of their main concerns.

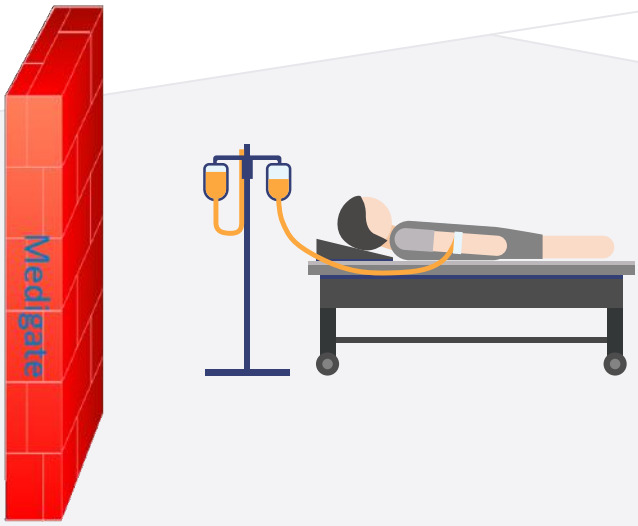
> **The truth is that many medical device manufactures' applications are vulnerable, since during their development and pre-market process, security is not necessarily their sole consideration.**

The truth is that many medical device manufacturers' applications are vulnerable, since during their development and pre-market process, security is not necessarily their sole consideration.

Additionally, COTS operating systems may pose a particularly worrisome problem, as they are more common, easily accessible and rarely patched.

To sum up, in contrast to the IT world, in which the vulnerability patching process tends to be fast and agile, the world of medical devices exposes a much more complicated challenge. Vulnerabilities remain unexposed for longer times. Even as they are found, the process of creating a security update demands comprehensive software testing, adaptation to the specific medical device. These dynamics, along with the challenges around HDO/manufacturer communication, create a cumbersome process that gives cyber criminals ample opportunity to mount attacks against medical devices.

This situation demands that we evolve from a traditional reactive approach to a proactive one. We must begin looking for the threat not only at the end points, where it might already be too late, and consistently place our guards within the medical networks. This will help us to preempt attacks and gain an advantage over the malicious actors in the space.



This is exactly where Medigate comes into play. Medigate's Medical Device Security Platform (MDSP) provides HDOs with superior visibility into their clinical networks by generating the exact make and model of all the connected medical devices. Visibility ensures that IT and Biomed personnel are informed of the current connected medical device inventory and it's respective technical networking specifications (OS, MAC, Firmware, etc.). This in-depth knowledge will alleviate the difficulties of the patch management process as it empowers HDO CISOs and CMIOs to effectively communicate with manufacturers regarding potential vulnerabilities in their inventory.

Moreover, Medigate's MDSP detects unique clinical network anomalies and threats by employing Deep Packet Inspection (DPI) into the specialized medical device application layer protocols within the clinical networks. This advanced technique provides a medical contextual approach, fusing medical workflow knowledge with networking behavior, resulting in highly accurate detection capabilities.

Finally, Medigate's MDSP leverages the visibility layer to preemptively preclude cyber attackers from propagating throughout the clinical network by utilizing automated micro-segmentation, saving valuable FTEs from being used for the tedious manual labor otherwise required.

MEDIGATE

contact@medigate.io
www.medigate.io