WHITEPAPER

SYNOPSYS®

Establishing Secure Software Development Practices in Accordance with FDA Guidance

TABLE OF CONTENTS

Introduction

In what seems like the blink of an eye, humans have begun to merge with computers. Patient lives rely on pacemakers, insulin pumps, dialysis machines, and numerous other devices to augment organs or control vital body functions. In essence, these intelligent, computerized medical devices have become the equivalent of a vital organ that maintains life functions. Any failure in such devices can have catastrophic consequences for the patient as well as the manufacturer.

While the rapid advancement of medical technology has led to enormous healthcare benefits, it has also brought potentially life-threatening software issues that device makers must overcome. Like a vital organ, medical devices need continuous security and quality maintenance throughout their entire lifecycle, from inception to retirement. With the proper tools and clear staging gates along each phase of the software development lifecycle (SDLC), device manufacturers can establish secure software development practices that manage quality, security, and safety of medical devices in accordance with FDA guidance.

Evolution of software in healthcare

While software is used quite extensively in medicine today, traditional medicine depended on relatively simple, non-technical devices. Medical professionals largely relied on their experience and wisdom to provide patient care with basic tools. Over time, it became apparent that the use of software and associated technologies could dramatically increase the level of care provided, lower costs, and in many cases, improve patient experience.

Early software applications in medical systems and devices focused on automating and controlling processes that would otherwise require constant attention from healthcare professionals. Examples include the use of software to monitor life support systems or to alter medications and oxygen flow to patients. This allowed healthcare professionals to monitor and care for a greater number of patients and better manage human error.

As technology continued to grow in healthcare, software evolved to fully manage the most critical human "systems," an example being cardiac defibrillators. Implanted cardiac defibrillators deliver lifesaving shocks to patients during what the software detects as a state of potential trauma. Technologies like this have enabled patients to lead a relatively normal life despite having serious conditions that would have previously required constant attention to manage.

The tremendous healthcare benefits brought by medical technology has led to the hasty embrace of connectivity. Connectivity allows medical systems within a networked environment to interact with one another by wirelessly interfacing with the Internet, either directly and intentionally, or indirectly and unintentionally. However, the often unpredictable and sometimes hostile nature of network environments trigger system failures, introducing significant risk to critical day-to-day healthcare operations. As medical device connectivity continues to grow and evolve, it has become apparent that connected technologies come with significant risks to the safety and reliability of medical systems which manufacturers must be prepared to address.

Connected technologies come with significant risks to the safety and reliability of medical systems.

FDA attempts to address cybersecurity issues related to “connected” medical devices

The United States Food and Drug Administration (FDA) took early steps to address potential safety concerns related to connected technologies. However, the focus was on non-intentional misuse of medical devices. It was not until security researchers began exploring the intentional and potentially malicious misuse of communication technologies that the FDA and medical community began to consider implementing additional measures to assure continued safety and effectiveness of these new “connected” medical devices.

Addressing non-functional use (malicious misuse) of medical tools is an unfamiliar practice for the FDA. Throughout history, the focus of medical safety and effectiveness has primarily been from a functional perspective. When considering the intended use of a scalpel, for example, it is important to consider factors such as toxicity of metals used, but not whether a crazed patient could wield it as a weapon to stab people. Healthcare professionals are trained to properly secure the scalpel so it does not end up in the hands of a potential malicious user. However, in the case of connected medical systems, these conventions do not apply. Properly stowing away devices does little to prevent malicious misuse. Leveraging vulnerabilities within software, malicious users can discreetly and remotely infiltrate systems without physically having the system in their hands. As a result, it is vital to consider the security of medical systems from a non-functional perspective.

In June 2013, the FDA released a draft guidance titled “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices” to help medical device and system vendors address cybersecurity issues in connected medical technology. Some have criticized the FDA for taking this approach because complying with guidance is optional and despite years of research and discussions, device manufacturers still continue to fall short of the mark when it comes to addressing basic cybersecurity issues.

Below are several examples of medical systems and devices still in use today with numerous known vulnerabilities:

Figure 1.1 illustrates the overall risk posture of a hospital monitoring system. The monitoring system contains over 1,600 known vulnerabilities, with over 300 in Java alone.

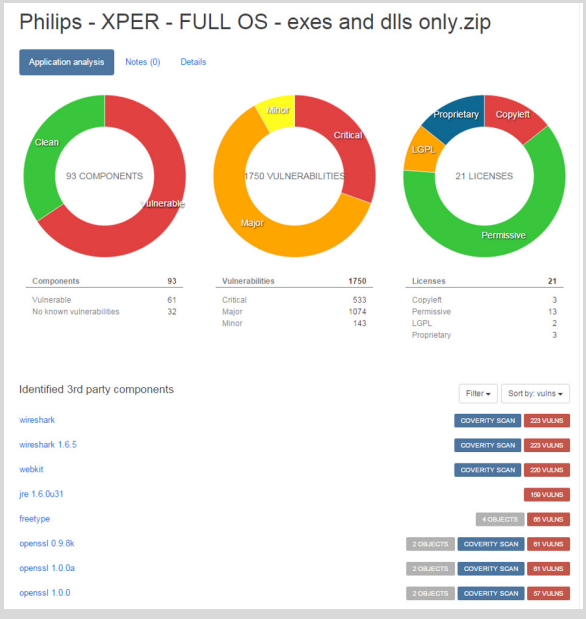

Figure 1.1

Figure 1.2 (below) provides proof that these vulnerabilities are not limited to a specific niche in the medical ecosystem; a wide variety of systems and devices contain known vulnerabilities, including implantable devices, monitoring and diagnostic tools.

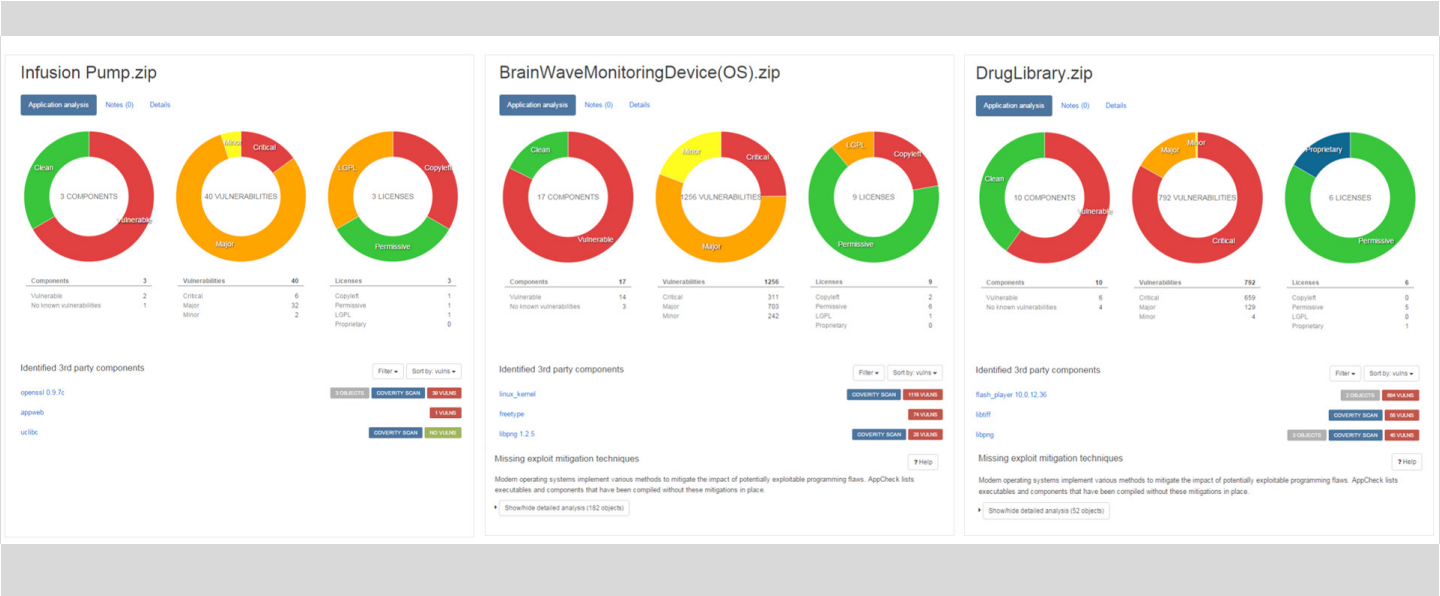

Figure 1.2: Protecode Supply Chain™ reveals that a random infusion pump contains 40 known vulnerabilities, a random brain wave monitoring device contains 1,256 known vulnerabilities and 182 missing exploiting mitigation techniques, and a random drug library contains 792 known vulnerabilities and 52 missing exploit mitigation techniques.

When considering these cases alone, it becomes clear that guidance alone is not sufficient.

In July 2013, the FDA moved toward setting an appropriate tone for device manufacturers by building a cybersecurity testing lab. The FDA recognizes the need to expand its role with respect to cyber security audits and has stated they are arming themselves with knowledge and capabilities both as a precedent and for the purpose of potential internal testing and verification. Such internal testing may be performed in cases where the FDA feels that a device poses a high cybersecurity risk, or when a device manufacturer is unable or unwilling to submit adequate documentation.

The bottom line is that the FDA is taking cybersecurity very seriously and expects medical device manufacturers to do the same. Device manufacturers should familiarize themselves with tools and auditing practices that help improve medical system security. Eventually, it is expected that the FDA will require testing methodologies as a part of the sign off process for medical device approval, allowing both the FDA and the healthcare industry to better manage cybersecurity issues.

Securing medical devices

All medical systems and devices have software running on them. Developing secure software is integral to the overcoming cybersecurity issues because insecure code is often the cause to system failures and breaches. However, uncovering the many different ways to cause system failures or infiltrate a device is a huge challenge. Unintended or malicious use is an infinite space problem. There are literally an infinite number of ways to misuse a device. Because products must eventually ship, it is not practical and nearly impossible to spend an infinite amount of time testing for security issues. The best tools are ones that can effectively “shrink” infinity to a manageable number of common misuse classes along your secure development lifecycle (SDL).

Automated tools, both commercial and open source, are available to facilitate the creation of secure software. The list below is not a survey of available tools; instead, it is an introduction to the types of tools that are available.

Static Code Analysis. This consists of examining source code (or an intermediary of source code) to look for defects that can lead to failures. Originally developed to address functional failures, as static code analysis has evolved it has become an effective method for enumerating security flaws, particularly commonly encountered software weakness types known as Common Weakness Enumerators (http://cwe.mitre.org). The FDA has strongly recommended the use of static code analysis for functional development and can indeed extend this to include non-functional weaknesses.

Software Composition Analysis. This testing methodology is absolutely critical due to the fact that an estimated 70% to 90% of software applications today use third-party libraries. Static code analysis requires access to source code and compiled third-party software components do not always readily provide access to source code. By applying software composition analysis techniques to compiled binaries, the third-party components can be determine, and checked against various databases of known vulnerabilities, such as the NIST National Vulnerability Database (https://nvd.nist.gov) to determine common vulnerabilities and exposures (CVEs).

Fuzz Testing. This method is highly effective in discovering unknown or "0-Day" vulnerabilities. The fuzz tester interacts with the running system via its external interfaces, providing a sequence of carefully chosen inputs in an attempt to trigger bad behavior. In some tools, the malformed inputs can be captured and replayed to produce consistent failure modes, which software developers can correct. The FDA recommends that device manufacturers include fuzz testing as one of several means of discovering cybersecurity-related vulnerabilities and uses the Synopsys fuzz testing tool (Defensics), a fuzz testing tool, in their cybersecurity testing lab. While there are multiple fuzz testing tools available, it is critical that the selected tool test as many of the protocols supported by a device as possible.

The most effective tools are the ones that produce repeatable results and quantifiable metrics for auditing purposes. Device manufacturers can audit their security posture by establishing metric-based gating criteria along each stage of the SDLC and verify testing results against those criteria. Implementing stage gates allows management to gauge the state of the overall development project not only in terms of "number of features completed," but also in terms of quality and security. Developers also benefit from clear guidance on how to prioritize efforts and resources, ensuring that the most critical security issues are addressed as they rise, before they lead to system failures. Overall, a process of continual verification helps organizations meet security standards without slowing productivity.

The most effective tools are the ones that produce repeatable results and quantifiable metrics.

Wrap up

The FDA is taking cybersecurity very seriously and it is highly advised that device manufacturers do that same. Device manufacturers are encouraged to familiarize themselves with tools to establish secure software development. Creating secure software development processes across an organization, while challenging, is achievable with a set of automated tools and proper stage gates along the SDLC. Tools such as static code analysis, software composition analysis, and fuzz testing effectively produce repeatable results and quantifiable metrics for auditing purposes, a recommendation consistent with FDA guidance. Using these tools and establishing criteria based gates along the SDLC help reduce cost and schedule risk, without compromising on time to market.

Find out how Synopsys can help you secure your software development practices in accordance with FDA regulations.

Learn more.

THE SYNOPSYS DIFFERENCE

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software

SYNOPSYS®
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com