Shedding Light on Medical Device Security

Using fuzz testing to mitigate risk inherited by medical device manufacturers.
Abstract

Healthcare providers are utilizing technology throughout their enterprise to not only provide the utmost patient care, but to also meet stringent requirements administered by the National Institutes of Health (NIH) and the Food and Drug Administration (FDA). While the advancement and use of medical technology have led to tremendous healthcare benefits, they also come with alarming security, quality, and safety concerns.

This case study documents a leading healthcare provider’s use of fuzz testing to mitigate risk inherited by medical device manufacturers.

Solution evaluation

The number of connected devices in hospital systems continues to grow at a rapid pace in order to improve patient interaction, reduce overhead, and minimize errors. One of the nation’s leading providers of advanced healthcare sought to ensure the hospital selected safe, secure, and quality technology in the hospital network by establishing meaningful security metrics for procuring new medical devices and a formal baseline for the current fleet of devices in use.

In order for the healthcare provider to define meaningful metrics, they needed a tool that provides insight into the risks inherited by medical devices. The hospital chose the Synopsys fuzz testing tool (Defensics) as the primary testing tool for evaluating device security. The hospital wanted a powerful yet simple-to-use tool that allowed them to quickly test and evaluate numerous devices without compromising patient safety or patient health information (PHI). Because the Synopsys fuzz testing tool requires minimal monitoring and provides real actionable insight into problems with low false negative and false positive rates, it enabled the hospital's security group to properly prioritize time and resources during testing.

The Synopsys fuzz testing tool employs black-box testing techniques, meaning it doesn't require any source code, to provide users with a comprehensive vulnerability assessment. This feature was particularly intriguing to the healthcare provider because it allowed the hospital's security group to approach manufacturers with detailed information on the devices' network-based vulnerabilities during the product evaluation phase of the purchasing process. The healthcare provider saw value in obtaining comprehensive visibility into the security, quality, and safety of medical devices, helping the hospital to make informed risk decisions.
Deployment and benefits realized

Information gathered during testing highlighted a high number vulnerabilities that could trigger potential denial of service (DoS) attacks. By utilizing the Synopsys fuzz testing tool, the healthcare provider has been able to minimize the potential for mass DoS events, ensuring patient care and patient safety.

Fuzz testing also simplified communications between the healthcare provider and their manufacturers. Clear concise reports containing Common Weakness Enumeration type, anomalies payload, and specific message segments, enable manufacturers to quickly find and remediate error conditions and allow the healthcare provider to effortlessly confirm devices meet internal security standards.

Most importantly, the healthcare provider is enabled to make informed risk decisions based on the information provided by Synopsys. While the healthcare provider can request for a fix during the procurement process, patches and updates from the manufacturers must go through a rigorous testing process that can take months before a patch is released. These are critical factors that the healthcare provider must weigh in when making purchasing decision from a patient care and patient safety standpoint.

As a result of using the Synopsys fuzz testing tool, the healthcare provider has been able to:

- Enhance purchasing decision by including security metrics
- Reduce testing effort
- Minimize impact to patient care
- Enhance patient safety

Conclusion

As modern healthcare continues to grow more dependent on technology, device robustness will become a critical aspect of the purchasing decision for medical devices. Ongoing use of fuzz testing throughout the medical device life cycle will ensure that healthcare providers stay abreast of new and emerging vulnerabilities introduced during updates and products enhancements. By demanding safe, secure, and quality medical technology, healthcare providers are setting a higher standard for patient care and patient safety across the industry.

Explore how the Synopsys fuzz testing tool can improve your medical technology.
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