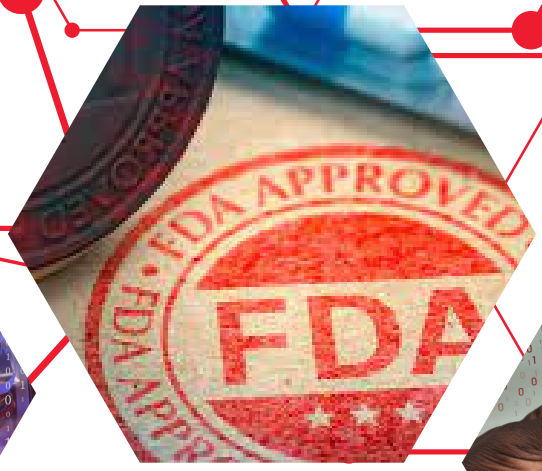

CODESECURE

PRODUCT SECURITY GUIDANCE FOR MEDICAL DEVICE MANUFACTURERS

Overview:

The FDA issued a final guidance document in September 2023, entitled “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions”. The document covers many aspects of device security and software security best practices including the role of software bill of materials (SBOMs) as a vehicle for risk management. The FDA has taken a broad approach to defining software to include “device manufacturer-developed components, including purchased/licensed software and open source software…” The FDA recommends that any premarket submissions include SBOM documentation for this software.

How a medical device manufacturer complies with the guidance will of course be up to them. However, the guidance presents significant and unique challenges to the software development teams that this document will discuss.

Challenges with Current Approaches to Generating SBOM

- Software bills of materials (SBOMs) have traditionally been produced during the development cycle using SCA tools with source code as the input to the tool. However, the FDA guidance stipulates SBOMs will be required from all device software, some of which will only be available in binary form. Consequently, source SCA tools don't provide a comprehensive SBOM as required by the FDA Guidance. Source-based Sourceoes not cover 3rd party binaries, purchased and licensed software which includes:
  - Operating systems
  - Remote Management Software
  - Communications Software
  - Platform Infrastructure (Software Libraries)
- Source scanning will miss binaries included as part of the build process
- How do you detect calls to external dependencies such as DLLs and shared libraries
- Most software vendors MSFT are unwilling to provide an SBOM, and even if they did would you trust it?
- Other software elements that are not shipped will be reported

A Fresh Approach: Binary Composition Analysis (BCA)

There are now software composition analysis applications in the market that can analyze binary code – these binary composition analysis (BCA) applications can be a key to complying with the FDA guidance.

Generating SBOMs in a post-production cycle produces favorable outcomes such as:

- Detailed operating system version detection including hotfix level. Large numbers of vulnerabilities are reported against operating systems, such as Windows 10. However, Windows updates are continually addressing these vulnerabilities, to understand what vulnerabilities truly affect the underlying operating system, the precise hotfix/patch level of the operating system needs to be detected and reported. CodeSentry can report the precise version of the operating system, including the hotfix level. Reporting included components in the device software “As deployed", confirms that the latest versions of 3rd party software are correctly included in the software
- Covers all binaries that are executing on the device, as well as redundant or unnecessary components that may be shipped with 3rd party software and could still be exploited
- Source SCA during SDLC costs developer time, and still doesn’t cover 3rd party binaries
- Confirms the proper setting of compiler flags and options that improve the security of the compiled application (Security Attributes)
- Using a BCA application a complete SBOM (component and version) of the open source component of the system can be presented to the FDA as part of device certification.
- CodeSentry from CodeSecure is the BCA solution that provides the comprehensive binary analysis required to help meet the FDA guidance.

For more information please visit:
www.codesecure.com