BlackBerry | QNX

PRINCIPLES AND PRACTICES FOR MEDICAL DEVICE CYBERSECURITY

MEDICAL DEVICE CYBERSECURITY IS OF GROWING CONCERN

[Credit the U.S. FDA, 2021]

Manufacturers must address cybersecurity risk.

Software supply chain security is essential.

Devices need to be secure throughout the product lifecycle.

A SECURE MEDICAL DEVICE REQUIRES:

- Company Culture
- Defense in Depth
- Understanding of Software Composition
- Secure Supply Chain
- Secure Connectivity
- Continuous Secure Updates

BUILD A SUCCESSFUL SECURITY CULTURE WITH THE HELP OF:

PROCESS STANDARDS

TIP: Adopt and adapt process models, such as the NIST Cybersecurity Framework.

GAP ASSESSMENT

TIP: The gap assessment is best performed by an external security consultant with medical device expertise.

- Well-Defined Internal Processes
- Executive Endorsement
- Company-Wide Buy-In

IDENTIFY ATTACK SURFACES

ATTACK SURFACE

Network insecurities	Software bugs	Physical security loopholes	People prone to social engineering
Open ports *Weak protocols*	*Insufficiently secured in-house-developed applications* *Vulnerable commercial programs*	*Rogue or dissatisfied current and former employees* *Openly displayed login credentials (e.g., username-password combinations on sticky notes, etc.)*	*Reused or recycled passwords* *Unmonitored use of social media and unprotected personal devices*

TIP: Attack surfaces are like safety hazards; mitigating them starts with design requirements.

SHRINK ATTACK SURFACES THROUGH:

- *RUN-TIME ISOLATION*
- *COMPUTE RESOURCE ISOLATION*
- *MEMORY SEPARATION*
- *PROCESS PRIVILEGE CONTROL*

TIP: A microkernel OS or hypervisor strengthens device security. The kernel is separated and isolated from the memory space used by other components, such as drivers. Each component runs in a dedicated memory space and cannot use the memory space of another component.

SELECT OFF-THE-SHELF SOFTWARE COMPONENTS BASED ON:

- Supplier Track Record
- Product Information
- Compliance With Standards Such As IEC 62304
- Supplier Audit from Product Lifecycle to Product Artifacts
- Vulnerability Scan of Compiled Binaries

TIP: Read the FDA guidance document, *Off-the-Shelf Software Use in Medical Devices*

CREATE AN SBOM OF ALL SOFTWARE USED TO CREATE THE DEVICE

- Proprietary
- Commercial
- Open Source

TIP: Software composition analysis technology creates SBOMs automatically, an otherwise massively time-consuming task when undertaken manually.

UNCOVER VULNERABILITIES IN THIRD-PARTY SOFTWARE AND IDENTIFY AREAS FOR SECURITY HARDENING AND REMEDIATION

FACT: Cybersecurity testing of the device software, including OSS, is the responsibility of the medical product manufacturer — not the suppliers!

TIP: Use a cybersecurity analysis solution designed for complex and critical embedded systems like medical devices to scan the compiled binaries of a complete software product for vulnerabilities and software craftsmanship.

ENSURE SAFE DATA COMMUNICATION AND CONNECTIVITY

Connectivity creates an attack surface.

Attacks increase as more devices are connected.

FACT: There were 2.5 billion malware attacks, 305 million ransomware attacks and 32.2 million IoT malware attacks globally in the first half of 2021.

Source: 2021 SonicWall Mid-Year Cyberthreat Report

TIP: A black channel approach based on the IEC 61508 standard enables safe communication between endpoints, even through an unsafe communication stack.

PLAN FOR SOFTWARE UPDATES IN THE FIELD AS VULNERABILITIES ARE DISCOVERED

Use an over the air (OTA) solution that incorporates both security expertise and technology that uniquely identifies and authenticates both the source and target so you can securely update and manage endpoints.

TIP: With a microkernel OS can be updated in a more modular way than with a monolithic OS.

HOW BLACKBERRY QNX CAN HELP YOU:

- Adopt a deterministic, POSIX-compliant, microkernel real-time operating system
- Meet reliability and safety compliance requirements
- Secure embedded software over its deployed lifecycle
- Bring safe, secure products to market quicker, on budget and with quality

ABOUT BLACKBERRY QNX

Medical device companies globally trust BlackBerry® QNX® software for use in a broad range of life-critical and graphics-rich medical applications.

BlackBerry QNX provides time-tested and trusted foundation software, which includes the QNX® Neutrino® RTOS, a deterministic microkernel real-time operating system, a safety-certified OS for Safety and Hypervisor for Safety, along with cybersecurity solutions like BlackBerry® Jarvis® for software composition analysis and BlackBerry® Certicom® Asset Management System—all of which are purpose-built for embedded systems.

BlackBerry QNX also has the experts to provide the software, support and professional services you need to build better medical devices and get them certified and approved for market. We partner with you at every step, from the inception to the launch of your embedded system, and believe we are successful only when you are successful.