

Identifying Medical Device Vulnerabilities for Faster FDA Approval

Overview

A medical device manufacturer wanted to accelerate its time to FDA approval by reducing its attack surface and minimizing the severity of vulnerabilities in its devices—all without delaying product timelines or straining development resources. By running RunSafe's Risk Reduction Analysis, the company was able to quickly identify vulnerabilities in their software and see the potential effectiveness of RunSafe mitigations for protecting legacy devices without changing code or disrupting device performance.

Challenge

A medical device manufacturer needed to speed up FDA approval by reducing its device attack surface and minimizing vulnerabilities, especially in legacy systems.

With unpatched legacy devices posing cyber risks that could affect patient safety and delay approval, the company sought full visibility into all software vulnerabilities—including third-party components—to assess risk accurately.

To stay competitive and meet regulatory deadlines, they needed a solution that reduced risk without impacting performance or disrupting development workflows.



Industry

Medical Device



Key features

- **Vulnerability Analysis:** Identified exploitable vulnerabilities to support FDA approval and prioritize remediation efforts
- **Risk Mitigation:** Demonstrated how vulnerabilities could be mitigated without altering source code
- **Legacy Protection:** Revealed potential risk reductions by deploying runtime protection to secure legacy medical devices without requiring refactoring or rewriting

Solution

To help the manufacturer meet FDA expectations and reduce its risk posture, RunSafe Security conducted a comprehensive vulnerability analysis as part of its Risk Reduction Analysis.

Using the manufacturer's SBOM and associated vulnerability data, RunSafe identified and evaluated over 2,000 vulnerabilities present in the device. The analysis identified the vulnerabilities that posed critical risks, particularly those related to memory safety, and the risk reductions that could be achieved by applying RunSafe's runtime code protection to mitigate them.

About the Customer

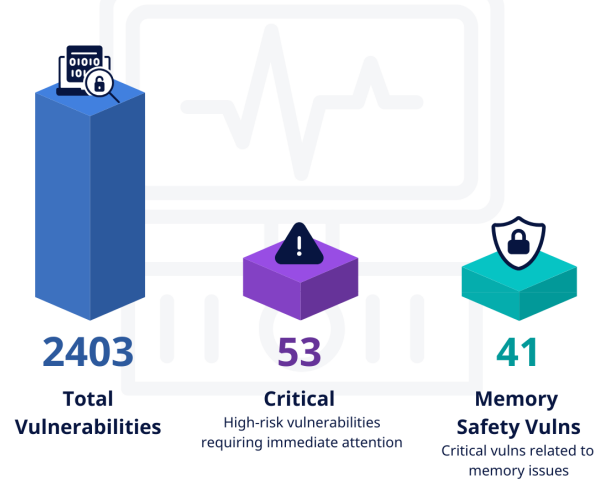
The company is a global healthcare provider that manufactures critical devices for patient care.



About RunSafe

RunSafe Security protects embedded software across critical infrastructure, delivering automated vulnerability identification and software hardening from build-time to runtime to defend the software supply chain and critical systems without compromising performance or requiring code rewrites. The RunSafe Security Platform includes the authoritative build-time SBOM generator for embedded systems and C/C++ projects, automated vulnerability identification and risk quantification, patented memory relocation techniques to mitigate memory-based vulnerabilities, and pre-hardened open-source packages and containers for immediate protection. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace and defense, energy, operational technology, industrial automation, transportation and automotive, medical device, and high-tech manufacturing verticals.

Vulnerabilities RunSafe Identified in a Medical Device



Of the vulnerabilities RunSafe identified, 53 were critical vulnerabilities, with 77% of those critical vulnerabilities related to memory safety.

Memory safety issues included:

- **CWE-119:** Improper Restriction of Operations within Memory Bounds (10 vulns)
- **CWE-120:** Classic Buffer Overflow (8 vulns)

RunSafe's Risk Reduction Analysis also demonstrated how software exposure could be reduced by applying RunSafe's runtime protections. For example, 49% of the vulnerabilities found in the device would be mitigated by applying RunSafe Protect, which would resolve 77% of critical vulnerabilities in the device.

Results

By running a RunSafe Risk Reduction Analysis, the medical device manufacturer received insight into total vulnerabilities in its device, the severity of vulnerabilities, and the potential to reduce risk in its software by applying runtime code protection.

With this information, the medical device manufacturer could make informed security decisions to:

Significantly reduce the device's attack surface.

Accelerate time to market for FDA approval.

Reduce developer time focused on manually chasing vulnerabilities, patching, and retesting.

Apply protection against both known CVEs and zero-day threats.