Medical Device Cybersecurity Use Case – RunSafe Security

Cyber Security

Challenge

- Our customer had a Medical Device in the market that needed a firmware update functionality.
- Given the high number of vulnerabilities, we looked for effective ways to significantly reduce the attack surface. These should not be intrusive to the development process and should not introduce risk.
- This was legacy equipment, which limited the patching to be done (updating the base OS was not an option).

Solution

- Critical Software partnered with RunSafe Security, a cybersecurity company with solutions to reduce the attack surface of critical systems.
- RunSafe brings security improvements related to the dependencies and other unknown memory vulnerabilities.
- We evaluated the effectiveness of RunSafe on the current list of vulnerabilities applicable to the SBOM of the device and identified a significant opportunity to reduce the current attack surface.

Benefits

- This improvement likely applies to all software versions, and both to the dependencies and the main application.
- **44%** of vulnerabilities were immediately mitigated after applying RunSafe technology (1057 / 2403).
- **71%** of most critical vulnerabilities mitigated (38/53).
- **100%** of Memory Safety vulnerabilities exploitable at runtime mitigated.