



embeddedTS Cyber Resilience Act (CRA) Support

embeddedTS is committed to helping our customers navigate the European Union Cyber Resilience Act (CRA) with confidence. As cybersecurity expectations continue to evolve, we are expanding our [Long-Term Support \(LTS\) program](#) to provide practical tools, guidance, and workflows that enable customers to create and maintain secure application deployments.

Our focus is on delivering flexible, real-world solutions that help customers meet CRA requirements without unnecessary complexity.

Delivered Through Our BSP and LTS Platforms

We are leveraging our [Yocto Board Support Package \(BSP\)](#) to enable customers to adhere to CRA requirements. Providing both platform support and reference images in a single Yocto layer to ease integration into larger applications with custom Yocto layers. Alongside this layer comes extensive examples and documentation, allowing our customers to fully own their workflow and integrate this support however they choose.

Support will be rolled out across our LTS platforms on a platform-series basis, connecting to our existing LTS software stacks to give our hardware platforms the best software support possible.

Secure Foundations from Boot to Deployment

embeddedTS will provide reference implementations for secure boot flows, enabling customers to establish a trusted chain of execution from system startup onward. These solutions ensure that only authenticated software is able to run on deployed systems, protecting against unauthorized modification and persistent threats.

Software Transparency with SBOM Support

To support CRA requirements for visibility and documentation, we will provide tooling and examples for generating Software Bills of Materials (SBOMs). Customers will be able to clearly identify all software components in their systems and maintain the documentation needed for compliance.

We will also provide guidance for vulnerability communication using existing tools such as [Dependency-Track](#), helping customers track vulnerabilities in their application and meet expectations of their customers for downstream reporting.

Secure and Flexible Update Strategies

embeddedTS will provide working examples and integration guidance for secure Over-the-Air (OTA) and offline update mechanisms using established frameworks such as [Mender](#), [RAUC](#), and [SWUpdate](#).

This approach allows customers to select and implement the update strategy that best fits their product requirements, without being locked into a single ecosystem.

Ongoing Vulnerability Reporting

We will provide direct vulnerability reporting for embeddedTS-maintained software, including our LTS Linux kernel, bootloaders, userspace utilities, and other platform components. This enables customers to respond quickly and maintain secure deployments over time.

Supporting Your Path to Secure Deployment

embeddedTS is committed to providing a strong foundation for secure, maintainable system design. By combining long-term platform stability with practical tools and proven workflows, we aim to give customers the flexibility needed to meet security and compliance requirements.

As cybersecurity regulations continue to evolve—including the introduction of new frameworks similar to the CRA—we will continue to expand and adapt our tooling, documentation, and platform support. Our goal is to ensure customers have consistent access to the resources needed to build, deploy, and maintain secure systems over time.