The Embedded Developer's Guide to the Cyber Resilience Act.

yocto PROJECT · EXEIN

TABLE OF CONTENT

yocto PROJECT · EXEIN

CHAPTER 1

Introduction to the Cyber Resilience Act

The Cyber Resilience Act represents a significant regulation that will affect embedded developers once enforced. It's important to understand its history, development, and the reasoning for its creation. Even though we expect it to kick in soon, specific details, such as penalties for non-compliance, are not yet defined.

This period serves as a preparation phase for embedded developers. Unlike other laws that mostly involve security teams or bosses, the Act needs developers to understand and get ready for what it means. This highlights the critical role developers play in compliance and enhancing cybersecurity in anticipation of the Act's official adoption.

The Growing Imperative for Cybersecurity

In the last few years, the online world has changed a lot, becoming more complicated and connected. Because of this, we need to keep our online information safe from people who want to attack it. The Act was created to help protect us from these attacks and make sure our online world stays safe.

Key Drivers for the Act's Genesis

Rising Cyber Threats: The reason for creating the Act is that there are more and more cyber threats happening, and they are becoming more advanced. Cyberattacks on important things like medical systems, factories, and other industries have shown that we need to deal with this problem quickly.

Global Interconnectedness

The Act recognizes that a breach in one area can have ripple effects, so it's important to strengthen cybersecurity in different fields. *Protection of Vital Systems:* Critical systems such as healthcare, energy, transportation, and industrial control systems rely more and more on embedded technologies. Keeping these systems safe from cyber threats is now a top priority.

The Act will impact embedded developers across multiple sectors and industries, with particular emphasis on two key areas: Critical Infrastructure and Industrial Control Systems (ICS).

Critical Infrastructure

This covers power grids, water treatment plants, and transportation systems.

Developers working on embedded systems in these sectors must follow the Act's cybersecurity requirements. Additionally, a third-party compliance assessment should be conducted to ensure thorough adherence and validation.

Industrial Control Systems (ICS)

Manufacturing plants, energy facilities, and other industrial sectors rely heavily on ICS. Developers in these domains must comply with the Act's requirements.

The Growing Imperative for Cybersecurity

In the last few years, the online world has changed a lot, becoming more complicated and connected. Because of this, we need to keep our online information safe from people who want to attack it. The Act was created to help protect us from these attacks and make sure our online world stays safe.

Key Drivers for the Act's Genesis

Rising Cyber Threats: The reason for creating the Act is that there are more and more cyber threats happening, and they are becoming more advanced. Cyberattacks on important things like medical systems, factories, and other industries have shown that we need to deal with this problem quickly.

Global Interconnectedness

Our world is more connected than ever.

The Act recognizes that a breach in one area can have ripple effects, so it's important to strengthen cybersecurity in different fields.

Protection of Vital Systems

Critical systems such as healthcare, energy, transportation, and industrial control systems rely more and more on embedded technologies. Keeping these systems safe from cyber threats is now a top priority.

The Act will impact embedded developers across multiple sectors and industries, with particular emphasis on two key areas: Critical Infrastructure and Industrial Control Systems (ICS).

Critical Infrastructure

This covers power grids, water treatment plants, and transportation systems. Developers working on embedded systems in these sectors must follow the Act's cybersecurity requirements. Additionally, a third-party compliance assessment should be conducted to ensure thorough adherence and validation.

Industrial Control Systems (ICS)

Manufacturing plants, energy facilities, and other industrial sectors rely heavily on ICS. Developers in these domains must comply with the Act's requirements.

Our world is more connected than ever

Technologies Covered

This Act covers a wide range of technologies, such as:

- **Embedded Systems:** The Act focuses on traditional embedded systems. Developers are responsible for ensuring that these systems meet cybersecurity requirements
- **Smart Devices:** The Act also extends to cover Internet of Things (IoT) devices, as they are increasingly common
- **Edge Computing:** Developers working on edge computing platforms are also subject to the Act's cybersecurity provisions

---

Important Provisions

Embedded developers must be aware of the Act's important provisions, as they directly affect their work.

Compliance Framework

The Act requires developers to:

- Assess cybersecurity risks
- Design products according to essential security requirements
- Ensure strong supply chain security measures

These requirements force developers to incorporate cybersecurity into their development processes and prioritize prevention and secure design principles.

Incident Response and Reporting

The Act focuses on responding to and reporting incidents:

- Developers must report security vulnerabilities and incidents quickly
- Working with cybersecurity organizations and market surveillance authorities is important for managing incidents effectively

These rules highlight how important it is to find and respond to threats quickly in order to protect digital products.

Future-Proofing and Adaptation

To future-proof embedded systems, the Act promotes:

- Following industry standards and best practices
- Preparing for new cyber threats
- Developers should evaluate and evolve development practices to manage new risks, ensuring the long-term security of embedded technologies

The Cyber Resilience Act significantly impacts embedded system developers due to its stringent cybersecurity requirements. To navigate embedded systems safely, developers should be well-versed with the Act's scope and key regulations.

CHAPTER 2

Objectives of the Cyber Resilience Act

1 / Promoting Cybersecurity

The Cyber Resilience Act aims to improve cybersecurity practices.
It recognizes that cybersecurity is important for national and international security, not just technology. This affects embedded developers in three main ways.

Security by Design

Developers are encouraged to make security a priority from the beginning of product development.

This means considering security at every stage, from design to deployment and maintenance.

Risk Assessment

The Act requires developers to assess cyber risks thoroughly. They must identify potential vulnerabilities and risks to ensure that their products can withstand cyber threats.

Continuous Improvement

Cybersecurity is always changing. Developers must keep up-to-date with new threats and adjust their practices to handle them.

2 / Safeguarding Data and Infrastructure

The Act acknowledges how important it is to keep both data and infrastructure safe. Just protecting data isn't enough - we also need to keep the systems that use, save, and send this data safe.

Keeping Data Safe

Developers need to make sure that data is kept private, accurate, and available. They should also make sure that sensitive information can't be seen by people who shouldn't see it, and use encryption where needed.

Protecting Infrastructure

Systems that are built into important infrastructure need to be kept secure so that things keep running smoothly. The Act reminds us how important this is, so that we don't have any serious problems.

3 / Standardizing Security Protocols

The Act aims to make cybersecurity protocols the same across different areas and businesses. This way, everyone follows the same rules.

Everyone Follows the Same Rules

Developers benefit from having clear, standardized cybersecurity rules.

These rules make it easy for developers to understand and follow the Act.

Different Systems Work Together

Same rules help different systems and technologies work together.

Developers can make solutions that work well with the cybersecurity rules.

Empowering Consumers

The Act wants to help people protect themselves from cyber attacks.

Consumer Protection

People should be able to use products that are safe from hackers. The Act wants developers to make security a priority so that people are safe from cyber threats.

Transparency

Developers must tell people how they're keeping their products secure. This will help people make smart choices.

Cybersecurity Education

The Act encourages people to learn about how to stay safe online.

Developers can help make these things happen by making sure they use good security practices, follow rules, and create safe products. If we all work together, we can make the internet a safer place.

CHAPTER 3

Implications for Embedded Systems Development

Design Implications

During the design phase of embedded systems development, the Act requires developers to focus on security.

Threat Modelling

Developers must identify potential vulnerabilities and threats through comprehensive exercises.

This helps in designing security features and defenses against specific risks.

Secure Architecture

The Act emphasizes the importance of secure architecture design.

Developers should incorporate security features such as access controls, secure boot processes, and encryption protocols from the beginning.

Data Protection

Protecting data is crucial.

The system's design should include encryption, data access controls, and secure data transmission protocols.

Development and Testing

The Act has a significant impact on the development and testing phases, including:

Secure Coding Practices

Developers must use secure coding practices to reduce the chances of security issues. This includes checking input, preventing buffer overflows, and handling errors correctly.

Testing Regimens

Developers must do thorough testing to find and fix security problems. This includes penetration testing, code reviews, and vulnerability scanning.

Documentation Requirements

The Act requires detailed documentation of the development and testing process so it's clear and traceable.

Deployment and Maintenance

When deploying and maintaining embedded systems, developers must follow certain considerations related to the Act.

Secure Deployment

Make sure to securely deploy embedded systems by focusing on secure provisioning, configuration, and updates.

Incident Response

Establish procedures to address security incidents and vulnerabilities after deployment.

Patch Management

The Act requires efficient patch management practices.

Ensure timely security updates and patches are applied to address newly discovered vulnerabilities.

End-of-Life Management

Even as embedded systems reach their end-of-life, the Act remains relevant.

Data Sanitization

Developers should delete sensitive data securely when retiring or disposing of systems to prevent data breaches.

Discontinuation Planning

Plans to retire or phase out systems should consider cybersecurity implications, including ensuring systems remain secure until final shutdown.

Regulatory Compliance

Regulatory obligations under the Act extend to managing systems at end-of-life, requiring developers to meet compliance requirements until retirement is complete.

The Cyber Resilience Act has significant technical implications for embedded systems development. Developers must consider security measures from the design phase, use secure coding practices, conduct thorough testing, and establish robust deployment, maintenance, and end-of-life management processes. These technical considerations are essential for ensuring compliance and enhancing the cyber resilience of embedded systems throughout their lifecycle.

CHAPTER 4

Compliance Checklist for Embedded Developers

1 Design Phase

Ensure security is included from the start

Use only secure and verified components

- Development Phase
- Use secure coding practices
- Ensure products shipped are vulnerability-free

2 Testing Phase

Add security testing to quality assurance

Supply the appropriate documentation

- Deployment Phase
- Roll out in a controlled environment
- Regularly check the code for vulnerabilities

3 Maintenance Phase

- Regularly update systems to fix known vulnerabilities
- Monitor for breaches and have a response plan ready

4 End-of-Life Phase

- Dispose of old systems properly
- Securely erase data so it can't be exploited

CHAPTER 5

Yocto Project Integration for Enhanced Cyber Resilience

Compliance Within the Yocto Project Build System

The **Yocto Project** is renowned for its robust build system, which facilitates the creation of custom Linux distributions for embedded systems. This system plays a crucial role in the development of secure products and applications. By using the Yocto Project build environment, you are taking advantage of shared collaboration and established best practices which meets a key requirement of the CRA.

Key Integration Points

Security Posture Analyzers

The Act underscores the significance of secure coding practices. To attain this goal, it is essential to incorporate a security posture analyzer into the Yocto Project build system. This integration facilitates ongoing security analysis, enabling the early detection of vulnerabilities during the development process.

Vulnerability Scanners

Regular scans for known vulnerabilities in software components are vital.

The Yocto Project can be configured to include vulnerability scanners, ensuring that only secure components are integrated into the build.

Proactive Defense

Use runtime security frameworks on your device to constantly monitor and quickly detect threats, keeping your systems safe and secure, even when offline.

Security Collaboration: Exein's Partnership with Yocto Project

In its role as a platinum partner of the Yocto Project and a trusted cybersecurity collaborator, **Exein** is joining forces with Yocto Project on a strategic mission. The goal is to improve the Yocto Project by making new security tools and technology accessible from its core. This aligns with the Yocto Project and the Linux Foundation's vision of promoting free and open-source software. By doing this, we can develop faster while adhering to established guidelines.

Advantages of Exein and Yocto Collaboration

Simpler Development: Developers can use community-validated, open source security tools that, combined with the foundational security provided by the Yocto Project, make secure application development less complicated.

Compliance Guarantee

Collaboration between Exein and Yocto ensures that your applications comply with security measures from the ground up, saving developers from the hassle of adding security measures after the fact.

Future-Proofing

With a core layer designed for security, developers can be sure that their projects will meet evolving cybersecurity regulations and challenges.

CHAPTER 6

Yocto Project Integration for Enhanced Cyber Resilience

In summary, the synergy between the foundational security offered by the Yocto Project build system and the expansive array of open source security tools, encompassing static code analyzers, vulnerability scanners, and security compliance checkers, establishes an ideal platform for crafting products that align with the requirements of the Cyber Resilience Act.

The partnership between Yocto and Exein aims to simplify secure application development while ensuring compliance.

This collaboration will help create strong, safe, and reliable embedded systems that can handle the constantly changing cybersecurity world.

We are working hard to make a security layer containing new tools and technology available to the Yocto Project community early next year working in conjunction with the tools already shared by Exein on GitHub.

About the Yocto Project

The Yocto Project is an open source project that enables developers to create custom Linux distributions for embedded and IoT devices. Supported by leading technology companies and developers worldwide, the project provides a flexible set of tools and a space where embedded developers can share technologies, software stacks, configurations, and best practices. https://www.yoctoproject.org

About Exein

Exein is a leading cybersecurity company specializing in providing advanced security solutions for embedded systems. Founded in 2018, Exein's mission is to safeguard the Internet of Things (IoT) and other embedded devices from growing cyber threats by offering innovative, integrated security solutions. https://www.exein.io

Appendices

Additional Resources and References:
https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act