MONTAVISTA SOFTWARE

Application

PRODUCT SECURITY BAD PRACTICES IN EMBEDDED LINUX SYSTEMS

Introduction

With a history of more than 20 years, **MontaVista Software** is proud to have empowered millions of devices across industries worldwide. Some of the world's leading companies, including Ericsson, Nokia, Mavenir and Grundfos have integrated **MontaVista's Carrier Grade eXpress (CGX) Linux** into their core technical system to utilize its design which emphasizes robustness, connectivity, and security in mission critical Telco Platforms, Medical Technology Systems, and Global, Resilient Industrial and Robotic Manufacturing environments.

The guidance document "Product Security Bad Practices" published by the Cybersecurity and Infrastructure Security Agency (CISA) in January 2025 presents product security bad practices that pose significant cyber threats for software manufacturers, particularly those serving critical infrastructure or national critical functions. For each unfavourable practice, they provide a description, recommended actions for risk mitigation, and relevant resources. We recommend you thoroughly review their document to understand the potential impacts to your environments.

This document from MontaVista outlines how we can relieve you of some of the product security issues specified in the CISA's guidance document. MontaVista's CGX Linux, along with MVSecure services, provides a framework for developing secure embedded systems.

Solution Description

According to CISA, the product security bad practices are categorized into product properties, security features, and organizational processes. As we examine each category one by one, we present how our solutions help you avoid the undesirable practices suggested by CISA.

Product Properties

1. Use of memory-unsafe languages
Developing new product lines in memory-unsafe languages like C or C++ when memory-safe alternatives are available is considered dangerous. For existing products, a lack of a published memory safety roadmap is also a significant risk. The roadmap should detail how a manufacturer plans to eliminate memory safety vulnerabilities in prioritized code components.

Our solution: MontaVista's CGX is built upon the Yocto Project and Linux kernel, and continuously updates to address known vulnerabilities, including CVEs. MVSecure services also help customers implement strong security measures and system configurations throughout the software development lifecycle, which will significantly assist in creating a memory safety roadmap.

2. SQL injection vulnerabilities
Allowing user-provided input to be directly included in a SQL database query string poses a serious security threat.

Our solution: MVSecure services can mitigate such vulnerabilities and offer solutions to avoid this bad practice in the software development lifecycle. SELinux can also be used to prevent unauthorized access to the database, even for the root user.

3. Command injection vulnerabilities
Having user-provided input directly into an operating system command string is dangerous.

Our solution: MontaVista's CGX Linux platform features a "Secure by Design" image with numerous security measures, such as secure boot, SELinux, and a comprehensive framework for managing security vulnerabilities and attacks. MVSecure services help customers address such vulnerabilities in software development lifecycle. Command injection is typically an application-level attack and a very common vulnerability found via the CVE mechanism. CGX makes sure you are always covered with the latest patches. Additionally SELinux can provide another layer of defence in depth for compromised applications, limiting the damage they can do in the system.

4. Default passwords
Releasing a product with default passwords that are universally shared and not required to be changed is a critical risk.

Our solution: MontaVista's CGX supports password security by various built-in features, such as Trusted Platform Module 2.0 (TPM 2.0) and OpenSSL (FIPS mode). Our Secure-by-Default profile also comes with predefined password settings. MVSecure services can assist customers in implementing strong authentication mechanisms that eliminate this bad practice.

5. Known exploited vulnerabilities (KEVs)
Releasing a product with components containing vulnerabilities listed in CISA's KEV catalog is dangerous. Not patching new KEVs in a timely manner is also considered a critical risk.

Our solution: The standard license of MontaVista's CGX Linux provides continuous security patches and bug fixes aligned with the Yocto Project LTS releases and known vulnerabilities (CVEs) in its SDK build system. These updates are validated through our robust QA infrastructure. In our latest release, CGX 5.0 is equipped with an update mechanism that is based on The Update Framework (TUF) and allows NSA-backed security for delivering over-the-air updates (OTA updates) to running targets.

6. Open source software vulnerabilities
Including open source software with critical vulnerabilities in a product at the time of release is a high risk. Failing to patch newly discovered vulnerabilities in the released open source components is also dangerous.

Our solution: In the Secure-by-Default profile, MontaVista's CGX provides modern tools for generating and managing SBOMs, which helps customers manage transparency and compliance related to component trustworthiness in the open-source software supply chain, such as the US Executive Act on Cybersecurity. The built-in mechanism for scanning and reporting CVEs also allows customers to mitigate vulnerabilities and potential risks efficiently.

7. Insecure cryptographic algorithms or lacking encryption
Using known insecure or deprecated cryptographic algorithms or inadequate encryption for transmitting or storing sensitive data is a serious risk.

Our solution: MontaVista's CGX offers built-in features, including TPM 2.0 and OpenSSL (FIPS mode), that help you avoid this bad practice. In the Secure-by-Default profile, CGX provides out-of-the-box system configurations for secure cryptography and password setups. MVSecure services can assist customers in implementing modern cryptographic algorithms and secure data transmission protocols, ensuring compliance and future-proof protection for critical information.

8. Hardcoded credentials
Having hardcoded credentials or secrets in source code is a significant vulnerability.

Our solution: MVSecure services allow customers to mitigate such vulnerabilities and avoid the presence of hardcoded credentials in source code.

Security Features

9. Lack of multi-factor authentication (MFA)
IT products that do not support MFA, including phishing-resistant MFA, in their baseline version are considered dangerous. Not enabling MFA by default for administrator accounts is also a great risk. For some Operational Technology (OT) products, where MFA could introduce safety risks, manufacturers should employ other authentication measures and publish a threat model that describes their approach.

Our solution: MVSecure services allow customers to address such vulnerabilities, develop strong authentication setups, and build a threat model for their product security.

10. Insufficient logging for intrusions
Software products that do not provide sufficient logging capabilities for intrusion type detection, including configuration changes, identity and network flows (if applicable), data access and creation in the baseline version are dangerous.

Our solution: MontaVista's CGX Linux offers a variety of debugging tools, such as GDB (the GNU Debugger), KGDB, Strace, Wireshark, and LTTng2, which deliver effective logging ways and means of collecting evidence of intrusion types. The latest version (CGX 5.0) is also incorporated with Suricata IDS and Deep Packet Inspection (DPI) tools to protect interconnected networks from intrusion threats.

Organizational Processes and Policies

11. Failure to issue CVEs

Not issuing Common Vulnerabilities and Exposures (CVEs) in a timely manner, especially for critical or high impact vulnerabilities, poses serious security threats. Furthermore, not including the Common Weakness Enumeration (CWE) field in every CVE record is also a substantial risk.

Our solution: MontaVista is committed to issuing CVEs in a timely fashion. Our vulnerability handling policy is to quickly provide customers with necessary information, guidance, and security defect responses on time to minimize potential risks.

12. Lack of a vulnerability disclosure policy (VDP)

Not having a published VDP that includes the product in its scope is dangerous.

Our solution: Leveraging our extensive experience in CVE management, MVSecure services can help customers build a VDP for their products.

13. Unclear support period

For on-premises products, not clearly communicating the period of support is a significant risk.

Our solution: In the standard license of MontaVista's CGX Linux, we provide clear information about our long-term technical support and maintenance (+10 years), ensuring health and reliability of embedded systems and products throughout their life cycle.

Summary

This document has discussed MontaVista's solutions with reference to CISA's "Product Security Bad Practices" document. Our products and services are designed to help customers build secure, reliable, and compliant embedded systems for the long term.

If you are looking for an operating platform with high security, connectivity, and reliability, MontaVista's CGX Linux meets all of these demands and more. Additionally, MVSecure provides end-to-end security consulting and certification support services to achieve compliance with the latest cybersecurity certifications and standards, including the EU Cyber Resilience Act (CRA) and US Executive Order on Cybersecurity.

By leveraging MontaVista's deep expertise in Linux and quality offerings, you can reduce the risk exposure to the product security bad practices outlined by CISA!

Please visit www.mvista.com and/or contact us at sales@mvista.com or leaving a request for more information on our solutions.

MontaVista Software, LLC, is a leader in embedded Linux commercialization.

For over 20 years, MontaVista has been helping Linux developers get the most out of open source by adding commercial quality, integration, hardware enablement, expert support, and the expert resources of the MontaVista development community. Because MontaVista customers enjoy faster time-to-market, more competitive device functionality, and lower total cost, more devices have been deployed with MontaVista than with any other Linux.

For more information about MontaVista, visit http://www.mvista.com
Media Contact:
MontaVista Software LLC | E: pr-contact@mvista.com | T: +1 (669) 777-6841

**Linux® is a registered trademark of Linus Torvalds in the United States and other countries.*
MontaVista® is a registered trademark of MontaVista Software, LLC.
All other names mentioned are trademarks, registered trademarks or service marks of their respective owners.