CVE Management in MontaVista’s Long-Term Support

Overview

Common Vulnerabilities and Exposures (CVE) is a publicly accessible database of known security vulnerabilities in software or hardware, each of which is labeled with a unique identifier. The objective of the CVE is to promote the sharing of information about security issues to help enterprises assess their cybersecurity controls, strategies and potential risks, and upgrade their systems against the identified flaws.

It is worth noting that each CVE in the list does not indicate an assessment of severity. Organizations including MontaVista that maintain our own CVE lists typically have severity categorical ratings and/or numeric scores to the known vulnerabilities.

In today’s modern, connected world, security risks and defects continue to grow. The number of CVEs (29,004) disclosed in the first three quarters of 2024 has surpassed the record high of 28,000+ CVEs in 2023 and represents over 30% growth year over year (Source: Published CVE Records).

Growing CVE exploitations in Linux and OSS Supply Chain

Cybersecurity threats do not exclude Linux or any open source software (OSS) in modern software development. Linux operating systems and applications are estimated to have more than threefold increase in exploited CVEs. The majority of these CVE exploitations target servers and several devices based on *nix systems (Source: Kaspersky). Adding more complications, the complexity of the software supply chain has posed a wide range of challenges regarding how to effectively manage the risks associated with OSS components in software products.

As an example of a recent OSS supply chain attack, the multi-year open-source XZ Utils project was penetrated with malicious code by attackers who used multiple fictitious identities over 3 years to gain access. The attackers pressured the maintainer to add a co-maintainer, who then inserted a backdoor into the code, attempting to distribute it through major Linux distributions (Source: Kaspersky’s analysis of the backdoor in XZ).

Despite the explosion of vulnerabilities and cyber threats on the software supply chain, a good few companies selectively update the systems or leave some issues unresolved for years due to a lack of resources to patch their applications against all CVEs.

MontaVista’s CVE Management

As a leader in embedded Linux commercialization, MontaVista Software has long-standing experience in delivering secure Linux distributions across vertical markets. A key area in our high-quality long-term support and maintenance is comprehensive CVE management.

MontaVista’s team frequently provides security patches and bug fixes validated through our robust QA infrastructure. Our customers benefit from a secure OS environment without compromising their custom content and product development. Our vulnerability handling policy is to provide necessary information, guidance and security defect responses on time to minimize potential risks.

At MontaVista, we have observed a significant increase in our CVE records annually over the past decade, handled thousands of security vulnerabilities for our customers and prepared to address growing software supply chain security threats. Whether it is a new software update or a security patch, we always strive for an appropriate solution to mitigate critical security issues with full consideration of the customer’s long-term success.

Further information can be found in MontaVista’s security portal:

- CVE List and Response: https://support.mvista.com/Security/CVE/
- Vulnerability Response Policy: https://support.mvista.com/Security/PubPolicy/

In an effort to secure the software supply chain, we provide a scorecard that is built on the Open Vulnerability and Assessment Language (OVAL) and compatible with Tenable Nessus, CIS-CAT, and OpenSCAP scanners. This new feature aims to support transparency on component trustworthiness and compliance with regulatory frameworks, including the EU Cyber Resilience Act (CRA) and the US Executive Order on Cybersecurity.

Conclusion

Responding to CVEs requires a careful calculation. You must evaluate the seriousness of a CVE for your application, let alone considering the market regulations. While it is essential to avoid releasing code with serious known vulnerabilities, you probably do not want to have constant delays brought by unexpected CVEs.

With our deep expertise in embedded Linux and security from over 20 years, we can relieve you from this burdensome task. As part of MontaVista’s professional long-term support and maintenance, CVE management spans all our solutions, from Carrier Grade eXpress (CGX), MVEdge and MVShield products, to MVXpert and MVSecure services.

By partnering with MontaVista, you can reduce the risks associated with software supply chain security and focus on your value adding in product development.

To learn more, please visit our website www.mvista.com and/or get in touch with us at sales@mvista.com or leave a request.