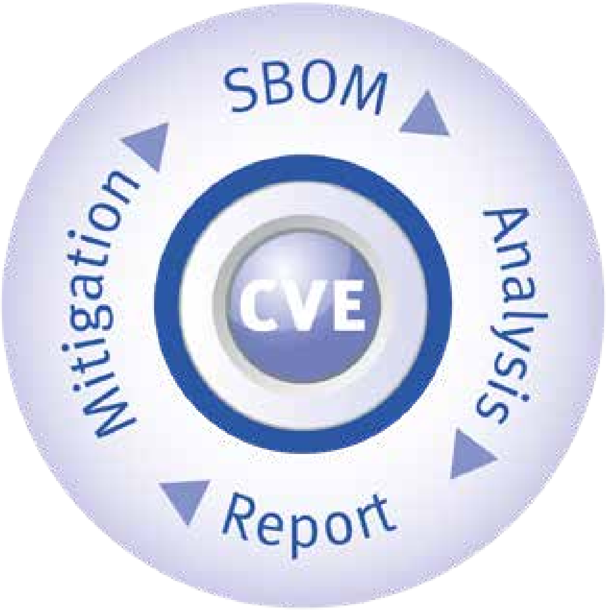
CVE Security Monitoring and Vulnerability handling

Lifetime product security – IEC62443, CRA/ TR-03183

Due to the Cyber Resilience Act (CRA) together with the Technical Guideline provided by the BSI (TR-03831) cybersecurity and security lifecycle maintenance became significantly more relevant for product design. This also applies for etstablished standards like IEC 62443 oder equivalent standards in other domains.

They all require product security to be an inherent part of engineering– from the very beginning („Security by Design“) to product disposal. And they all demand a continuous monitoring and management of all security relevant aspects throughout the whole product lifecycle. A security level once defined must be kept and it has to be possible to improve it due to new market requirements.



The „CVE or Vulnerability Monitoring“ as a part of the vulnerability handling makes sure that the system software – and herein the embedded Linux software - is continuously checked for up-to-dateness with regard to versioning, configuration and the integrated components.

This can be separated into four stages:

- SBOM (Software Bill of Material): Extraction of all included (OSS) components and integration for further stages
- Analysis: Identification of all applying vulnerabilities as well as the assessment of each finding with concerning relevance and its impact on the product security
- Reporting: documentation of the results
- Mitigation: identifikation and development of mitigations for all relevant vulnaribilities. Concerning open source software this is mostly patch- and update-management.

emlix CVE Security Monitoring supports you throughout the whole lifecycle of your embedded Linux based products.

SBOM

In case it is not provided by our customer emlix will generate a SBOM for all components and packages included in the system software. It will be created in compliance with IEC 5230:2020.

Analysis

The analysis consists of two steps.

- Monitoring: based on the SBOM emlix evaluates the National Vulnerability Database (NVD) and the Mitre Common Culnerabilities und Exposure Database in a widely automated process. Additional some further, sometimes even product specific sources are kept under surveillance.
- Assessment and contextualization: as required by the standards each finding will be assessed by emlix experts. In a first step package versions and configurations are taken into account. Even more important in a second step the relevance of each finding will be assessed concerning possible risks arising from the operatio-

nal and application context as well as the product's risk structure. Additionally the component specific exposure to vulnerabilities will be considered.

Report

- emlix will generate a CVE Security Report with a clear presentation of all security issues, mitigations and a recommendation for further steps (pdf or CycloneDX, VEX or SPDX). It is based on the monitoring and the subsequent expert assessment. It thereby provides valid content for supplier security compliance declarations (espacially concerning CVE monitoring, vulnerability handling as well as patch- and update- management). Upon customer's request the report can be made available via a Dependency Track instance hosted by emlix. It allows extended options for visualization and further analyses of SBOM and CVE data.
- Vulnerabilities, risks and mitigations will by discussed with our customer in regular meetings.

Mitigation

- Upon request we support our customers in release planning and update management. emlix embedded Linux experts prepare new releases with all relevant updates and patches as agreed with our customer. Sometimes ad hoc updates are required due to some severe security issue. Typically our customer will integrate regular updates in usual product care cycles.

Customer benefits

emlix CVE Security Lifecycle Management provides you with:

- maintenance of an initial product security level via con tinuous identification and assessment of vulnerabilities and mitigation measures.
- a highly efficient product and application specific risk assessment by experienced experts that leads to a significant cost and risk reduction during product maintenance.
- a transparent and understandable presentation and reporting of vulnerabilities, risks and mitigation measures with meaningful comments and recommendations.
- valid information for supplier security compliance declarations and reports as part of customer's vulnerability disclosure process
- planability of releases and updates
- an efficient and cost-effective feasibility.

The emlix CVE Security Lifecycle Management and – optional – the patch and update management is designed with respect to different standards and regulations and thus contributes to the compliance argumentation of your product with regard to cybersecurity.

Find out more. Our experts will be happy to provide consulting.

Phone +49 551 304460

solutions@emlix.com