VCode®
Supply-Chain Cybersecurity

Karamba Security

ISO/SAE 21434 and UN R155 are raising the bar for OEMs, requesting to verify suppliers' security posture and conduct continuous management of vulnerabilities in the OEM's deployed fleet.

Karamba Security's VCode software automatically identifies cybersecurity issues in suppliers' binaries, to comply with ISO/SAE 21434. The software automatically scans third-party and internally developed ECU binaries and identifies the software bill of materials (SBOM), as well as security vulnerabilities, misconfigurations, authentication glitches and risky tools.

VCode's Vulnerability Management System continuously receives new vulnerability data, and prioritizes its handling, based on automatically generated blast radius reports and vehicle SBOM.

Karamba Security VCode stands out as the industry's leading binary analysis tool with its deep technology advantages:

Coverage

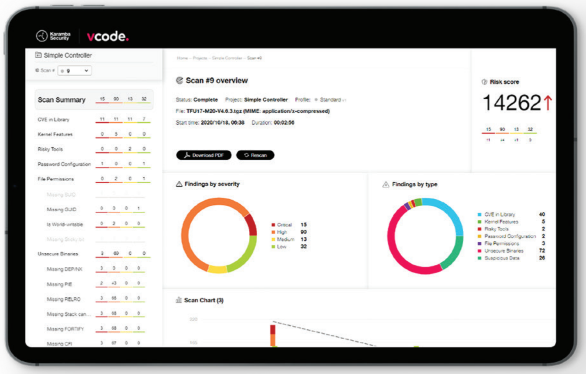
- OS: AUTOSAR, embedded Linux, QNX, Android
- Cybersecurity issues: CVEs, risky tools, misconfiguration, outdated credentials, embedded URLs, weak passwords
- All issues are discovered throughout the supply chain

Speed

- Karamba's VCode is super-fast. It scans 100MB/min to allow a streamlined verification process, without forcing delays or changes in development and integration pipelines
- VCode highlights security issues immediately after the ECU scan, prioritizes findings and suggests mitigations

Simplicity

- VCode operates an easy-to-use user interface, which enables even the most overwhelmed product security team to identify security issues in the ECU binaries, without needing to learn the tool or read extensive user manuals
- VCode connects to the CI/CD pipeline in order to automatically scan each new software release, without requiring cumbersome analysis processes for each version and sub-version
- Karamba's Vulnerability Research team may support you during the scan and can advise appropriate actions to mitigate VCode findings



Scan #9 overview

Status: Complete Project: Simple Controller Profile: Standard

File: TFU17-M20-V4.6.3.tgz (MIME: application/x-compressed)

Start time: 2020/10/18, 06:38 Duration: 00:02:56

Risk score

14262↑

Scan Summary	15	90	13	32
CVE in Library	11	11	11	7
Kernel Features	0	5	0	0
Risky Tools	0	0	2	0
Password Configuration	1	0	0	1
File Permissions	0	2	0	1
Missing SUID	[illegible]	[illegible]	[illegible]	[illegible]
Missing GUID	0	0	0	1
Is World-writable	0	2	0	0
Missing Sticky bit	[illegible]	[illegible]	[illegible]	[illegible]
Unsecure Binaries	3	69	0	0
Missing DEP/NX	3	0	0	0
Missing PIE	2	43	0	0
Missing RELRO	3	66	0	0
Missing Stack can...	3	68	0	0
Missing FORTIFY	3	68	0	0
Missing CFI	3	67	0	0

Findings by severity

Critical	15
High	90
Medium	13
Low	32

Findings by type

CVE in Library	40
Kernel Features	5
Risky Tools	2
Password Configuration	2
File Permissions	3
Unsecure Binaries	72
Suspicious Data	26

Karamba Security

Binaries from Any ECU

VCode is an open platform that scans and analyzes binaries from any ECU system: AUTOSAR based RTOS from Vector and Elektrobit, embedded Linux, QNX and Android systems

Wide Range of Findings

VCode highlights oversights with detailed, explainable, findings: known and unknown vulnerabilities in the software, compiler and linker security misconfigurations, weak or empty passwords, embedded credentials, and more.

Multi-Tiered Supply Chain

By scanning final deliverables in a multi-tiered production process, VCode tracks and exposes both internal and third-party components, shedding light on the supplier capabilities as required in section 7.4.1 of ISO 21434

Simple to Use

Easily integrated into the CI/CD pipeline, binaries are loaded to the VCode engine without interfering with the development process. With its scanning speed, OEMs can integrate VCode into the FOTA process, to assure security quality of the updates

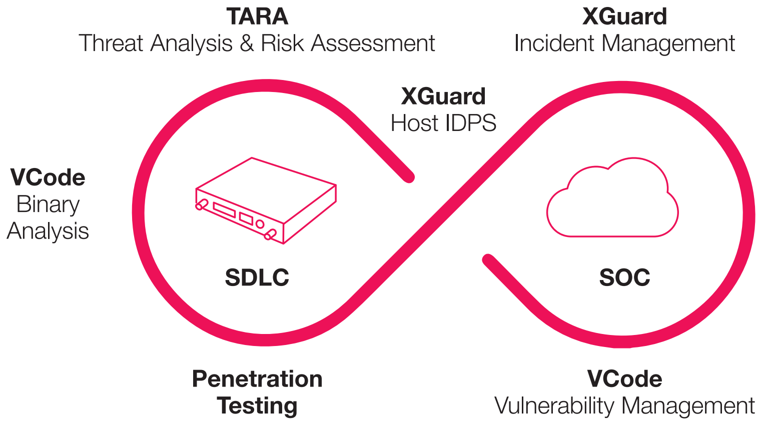
SBOM Management

VCode provides OEMs with complete visibility of SBOM components, including third-party libraries, and can export/import them in CycloneDX and SDPX formats

Standard-based Reports

VCode's vulnerability scanning identifies and prioritizes security issues according to ISO/SAE 21434 guidelines and UN R155 Appendix 5 mitigations, saving time in last-minute pentests

Karamba's End-to-End Product Security



TARA
Threat Analysis & Risk Assessment

XGuard
Incident Management

XGuard
Host IDPS

VCode
Binary
Analysis

SDLC

SOC

**Penetration
Testing**

VCode
Vulnerability Management

Karamba
Security

Drive Innovation with Confidence

www.karambasecurity.com | contact@karambasecurity.com

Israel office Tel: +972 9 88 66 113
USA office Tel: +1 833 4KARAMBA
Germany office Tel: +49 172 3991 036