RUNSAFE SECURITY

From SBOM Visibility to Action:

A Reachability Analysis Checklist for Embedded Systems

WHY MOST SBOM-BASED VULNERABILITY LISTS ARE WRONG

Package-level CVE matching ≠ real exposure

Embedded builds only include a subset of source code

Teams waste time triaging irrelevant vulnerabilities

> "Many vulnerabilities flagged in scans are in code that was never compiled into your build."

Visibility	Action
"List of CVEs"	"Which CVEs actually apply?"
Package-level	File-level
Manual triage	Automated triage
Uncertain	Defensible (VEX-backed)

RUNSAFE SECURITY

REACHABILITY ANALYSIS CHECKLIST

☐ **Map vulnerabilities to actual compiled code**	• Validate which source files are included in the binary • Eliminate CVEs tied to unused code
☐ **Use build-time data (not post-build scans)**	• Capture file-level inclusion during compilation • Avoid relying solely on package manifests
☐ **Automate "Not Affected" classification**	• Apply **CycloneDX VEX** justifications • Document why vulnerabilities do not apply
☐ **Reduce false positives before prioritization**	• Remove irrelevant CVEs first • Then prioritize based on real exposure
☐ **Generate audit-ready evidence**	• Ensure traceability from: ◦ SBOM → file → CVE decision • Maintain repeatable, consistent outputs
☐ **Integrate into CI/CD**	• Run reachability analysis continuously • Keep vulnerability lists current with builds

WHAT TEAMS GET

- Reduction in triage workload
- Smaller, prioritized vulnerability backlog
- Defensible compliance posture (VEX-ready)
- Faster remediation of real risks

HOW TEAMS ARE DOING THIS TODAY

- Build-time SBOMs provide file-level visibility
- File-level visibility results in fewer false positives
- RunSafe's reachability analysis automatically triages
- Teams spend time on the CVEs that matter

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: **RunSafeSecurity.com.**

SEE HOW THIS WORKS IN YOUR BUILD PIPELINE