The RunSafe Risk Reduction Analysis

Analyze your exposure to CVEs and memory-based zero days and understand your total risk reduction potential.

THE PROBLEM

Memory-based vulnerabilities account for 70% of embedded software defects. Although these vulnerabilities have been a known issue for decades, they still persist today, putting legacy software and critical infrastructure systems at risk. The successful exploit of a memory-based vulnerability can lead to remote command execution, remote file manipulation, and more.

PROVIDING FULL VISIBILITY INTO CVES AND MEMORY-BASED ZERO DAYS

The RunSafe Risk Reduction Analysis gives you insight into total CVEs and exposure to memory-based zero days in your software. By understanding your exposure, you can take informed action to secure your embedded systems and eliminate the single biggest class of risk in embedded devices.

HOW IT WORKS

The RunSafe Risk Reduction Analysis, developed out of research from Linköping University, is designed to expose the risk to software from both **known and unknown vulnerabilities.** The analysis measures known CVEs based on SBOM ingestion or creation. The zero day analysis reveals unknown vulnerabilities by analyzing a binary for return oriented programming (ROP) chains.

For decades, ROP has been the go-to method for arbitrary code execution (ACE) attacks. Unlike traditional code injection, ROP works by reusing snippets of a program's own code to build a malicious payload, known as a ROP chain.

The RunSafe Risk Reduction Analysis reveals exposure to memory-based zero days in several stages. First it quantifies the number of binary attack vectors (or ROP chains) within software that can be used by the attacker for remote code execution, privilege escalation, or other unauthorized effects.

The analysis then measures risk reduction by analyzing exploit potential of **both known CVEs and zero days** before and after implementing RunSafe's patented memory relocation technology.

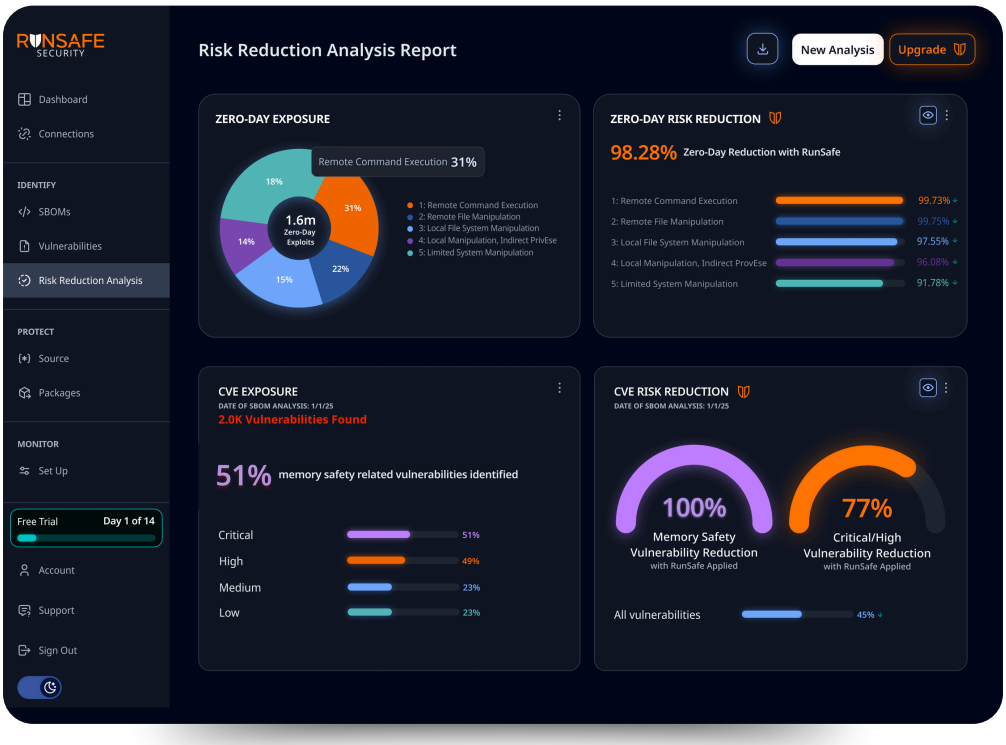
By significantly reducing the number of available devastating ROP chains—often to nearly zero—RunSafe minimizes the risk of code misuse attacks and strengthens software security.

START YOUR ANALYSIS

Step 1: Prepare a binary and/or SBOM you want to analyze to determine your risk exposure.

Step 2: RunSafe cyber experts will analyze your exposure to calculate the risk to your embedded systems.

Step 3: Get a score of your total exposure and risk reduction potential when runtime protections are applied.



MITIGATION WITH RUNSAFE PROTECT

RunSafe Protect mitigates cyber exploits by relocating software functions in memory every time the software is run, creating a unique memory layout that prevents attackers from exploiting memory-based vulnerabilities.

Unlike traditional ASLR, RunSafe's patented Load-time Function Randomization (LFR) provides more granular protection—without incurring additional runtime performance costs—allowing software to defend itself against both known and unknown vulnerabilities long after the last patch is available.

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.**