

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.

 Dushbaurd Connections CERO-DAY EXPOSURE Free friat Day 1 of 14 Account Support Support	RUNSAFE SECURITY	Risk Reduction Analysis Report	と New Analysis Upgrade 💓
 Connections Connections Solubic Vulnerabilities Solubic S	🔁 Dashboard		
 intrinie intrinie<			98,28% Zero-Day Reduction with RunSafe
 \$ StoMs \$ Vulnerabilities \$ Vulnerabilities \$ Stok Reduction Analysis \$ Packages \$ Packages \$ Packages \$ Stok Vulnerabilities Found \$ Stok Vulnerabilities \$ Stok Vulnerabilities \$ S	IDENTIFY	18%	
 Vulnerabilities Vulnerabilities Six Reduction Analysis Source Packages Account Support Sign Out Support Sign Out Sign Out 		1.6m 11.6m 11.6m 11.6m 11.6m	1: Remote Command Execution 99.73% 2: Remote File Manipulation 99.75%
 Risk Reduction Analysis Risk Reduction Analysis Froctett Source Rakages Rockages Rock Torkson Manipulation CVE EXPOSURE CVE EXPOSURE CVE EXPOSURE CVE EXPOSURE CVE EXPOSURE CVE ISS REDUCTION CVE EXPOSURE CVE ISS REDUCTION CVE I		14% Zero-Day Explaits = 0 3: Local File System Manipulation 4: Local Manipulation, Indirect PrivEse 5: Limited System Manipulation	3: Local File System Manipulation 97.55% *
PROTECT (a) Source (b) Source (c) Packages MONITOR (a) Set Up Status Day 1 of 14 (c) Critical High (c) Critical (c)	③ Risk Reduction Analysis	15% 22%	4: Local Manipulation, Indirect ProvEse 96.08% ♦ 5: Limited System Manipulation 91.78% ♦
PROTECT (a) Source (b) Source (c) Packages (c) CE EXPOSURE (c) Lot of SourANAUSSES INVES (c) CUE COSTON ANAUSSES Inves (c) Cue Coston			
A source Prackages Monitron Set Up 51% memory safety related vulnerabilities identified Critical Critical High 4 Account Sign Out	PROTECT		
Packages Montroe Set Up 51% memory safety related vulnerabilities identified Critical Critical High Stype of the formation of the form	(*) Source		
MONITOR © Set Up	🚱 Packages	CVE EXPOSURE : DATE OF SHOW MANAYSIS: 17/125 2.0K Vulnerabilities Found	CVE RISK REDUCTION
\$\$ Set Up Free Trial Day 1 of 14 A Account Critical High A Medium 23% Low 23% Low All vulnerabilities All vulnerabilities	MONITOR		
Free Trial Day 1 of 14 Account Critical High 19% Medium 23% Low 23% Low 23% Sign Out		51% memory safety related vulnerabilities identified	100% 77%
Account High 49% Vulnerability Reduction Medium 23% Ex Support Low 23% All vulnerabilities 45% +	Free Trial Day 1 of 14	Critical 51%	Memory Safety
Medium 23% Low 23% All vulnerabilities 45% -		High 49%	Vulnerability Reduction Vulnerability Reduction with RunSafe Applied with RunSafe Applied
Ex sign Out		Medium 23%	
E+ Sign Out	ι≂; Support	Low 23%	All vulnerabilities 45% +

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.

RunSafeSecurity.com