NETRISE

Data Sheet

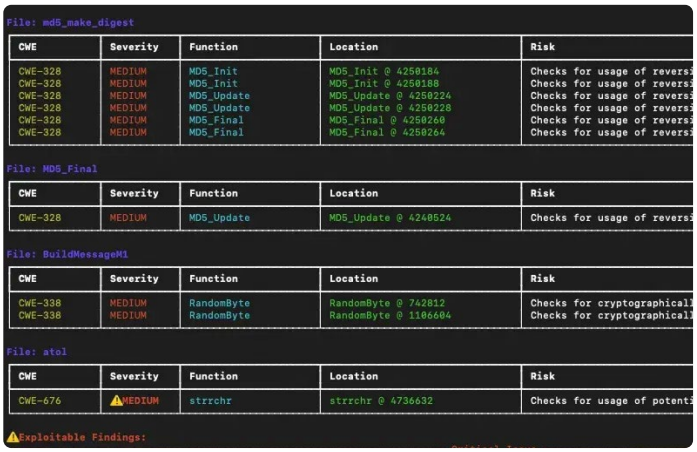
NetRise ZeroLens®

AI-Powered CWE Detection in Compiled Code

Find weaknesses before they become vulnerabilities

Why You Need NetRise ZeroLens

Many software weaknesses never make it to a CVE (Common Vulnerabilities and Exposures) database, but attackers find and exploit them anyway. ZeroLens helps you detect these CWEs (Common Weakness Enumerations) in compiled software before they turn into public vulnerabilities. Even when source code isn't available, you can gain visibility into undetected CWEs, verify patch effectiveness, and prioritize what to fix based on reachability and severity, all via binary analysis.



What You Can Do With NetRise ZeroLens

Binary Code Analysis

Scan compiled software and applications without source code.

CWE Detection and Remediation

Detect unsafe functions in binaries, map them to CWE categories, and generate remediation guidance.

Exploitability-Based Prioritization

Focus on weaknesses most likely to be exploited, not just those with high severity.

Portfolio-Wide Scanning

Process thousands of binaries in parallel to support full portfolio assessments.

Binary Patch Verification

Examine software updates to confirm that code fixes have been correctly applied.

Function Call Graphs

Generate call graphs that show how functions interact inside a binary, providing context for weakness analysis and downstream reachability efforts.

How NetRise ZeroLens Works

Input Formats

NetRise ZeroLens analyzes standard compiled binaries (ELF, PE, Mach-O). When used within the NetRise Platform, it also supports binaries extracted from firmware and custom images.

Outputs

CWE mapping, exploitability insights, severity scoring, and remediation recommendations

Reachability Analysis

Determines whether a weakness is present in an executable path to support exploitability-based triage

CWE Coverage

Focused on high-prevalence, high-impact software weakness categories

Deployment

Cloud-native, available via the NetRise Platform

Who Uses NetRise ZeroLens?

Product Security Teams (OEMs):
Detect weaknesses in software early in the development lifecycle..

Security Operations Teams:
Triage compiled assets and focus remediation on the most urgent findings.

Red teams and researchers:
Explore unknown weaknesses in third-party code missed by traditional static analysis.

Medical, critical infrastructure, or regulated industries:
Validate binaries in systems where secure coding standards are inconsistent or missing.

"NetRise ZeroLens gives us the ability to test software that other static analysis tools don't handle well. We use it to enforce CWE analysis where no secure coding standards exist."

Garrett Schumacher
Velentium Medical

See how NetRise ZeroLens strengthens software risk detection

Request a Demo

Learn more at: https://netrise.io/products/