



ObjectSecurity BinLens™ Automated Binary Vulnerability Analysis

ObjectSecurity[™] BinLens[™] 3.2

Automated Binary Vulnerability Analysis

Effortlessly uncover zero-day vulnerabilities in binaries with cuttingedge accuracy and minimal false positives.



Why:

- SBOM generation is limited to detecting only known vulnerabilities in published software.
- Source code analysis and static application security testing (SAST) produce too many false-positives, slowing down remediation.
- Network scanning fails in cases where devices are not connected to the network.
- ~20-70% of OT/ICS assets are end-of-life/legacy devices, lack source, or there are no patches.
- Talented reverse engineers are hard to find and manual reverse engineering is time consuming.

What:

- Unlock deeper security insights with BinLens[™] advanced binary analysis.
- Integrated approach combines multiple techniques to uncover potential zero-days with unmatched precision.
- Powered by automated symbolic execution, it excels at detecting memory-safety violations and other undefined behaviors in binaries, delivering a dramatically lower false-positive rate than competing tools.
- Automates key manual reverse engineering tasks like static analysis, disassembly, and decompilation.
- Primarily does not rely on known vulnerabilities.
- Flexible deployment—on-prem/offline or cloud.
- Supports 30+ CPU architectures, 50+ file formats.

ObjectSecurity[™] BinLens[™]



BALENS				
+	Default Facility -	Basa Symbolis CWCs Wesk Falmer		
88			All Values billion	
1 2 0 0	 Contains Symbolic Results Red miner bills and 			9 second(s) Analysis Complete
ø	Commercial Weak Pointers			
0		Detected Valuerabilities		
		Waterability		
	 D Fails Lineage Analysis Red 			
	· Others Painters			
	> C Test Maleure			
	> Chilberable Asset Example 1			
	> 🗷 Salipia Test Plan			
04,102	6 Copyright 2021 - 2024 Digentitienantly P	haven Delay	CPU Land 29. Interney 5 Byle / 119 GB 202 / 50000 Binaries	14 / 120000 Asserts 171.59 43 1 Tree Density

•	A Delucitarily -	ten into matteries front temperaturies and o					
					harden .		
	- Unit Despension				The PRCDFT function is not space in types 200 indices 1 kpc has an in-additional processing wavely apply, bandling is metrics unit association of an applicit in the restorable in the restorable metrics of a space ($R=0.000$ metrics) in an advance metrics of asympt ($R=0.000$ metrics) in a state metrics have applicable ($R=0.0000$ metrics) in the state metrics have applicable ($R=0.00000$ metrics) in the state metrics have applicable ($R=0.00000000000000000000000000000000000$		
	- (Mark Hanna	****			Starbin for the Foreignine Start (\$400), if and (\$400) and \$400 percent set of the set o		
	 Mil Microbiolitic Microbiolitic Microbiolitic Microbiolitic Microbiolitic Microbiolitic Microbiolitic Microbiolitic Microbiolitic 	01.00-00			$\approx \frac{1}{2} \frac{1}{2} \frac{1}{100} < \frac{1}{1000} < \frac{1}{1000} < \frac{1}{1000} < \frac{1}{10000} < \frac{1}{10000} < \frac{1}{10000} < \frac{1}{100000} < \frac{1}{10000000000000000000000000000000000$		
					10 (QUV(2)) 10 ag is Specific long (3.4) alone convext spectra to the square length to the line 10 (second length 10 (length) (leng		
		AL 101 Mar			and agent in Spacefills and an A. I has a shadk free that may be at the state of th		

	A Martiney -	 a Mainteen State Supportation Date -	
	- C Connected West Publics		
8 6		News a Antonially Designment Function	
0			
	- Children Hallen	American Citi	
	- Charles		
		Roard a Printing Despires Function	
	1 Charlenson		
	1 () March Sorthurgh 1		
	1 C Regis Test Has	Automation (M)	
	Concernance (
	- Wellington		
	· · · · · · · · · · · · · · · · · · ·		

Features:

- Stack Overflows: detect unsafe writes to the stack frame
- Heap Overflows: detect unsafe writes to dynamically allocated memory
- User Controlled Program Redirection: detect usercontrolled instruction pointers, arbitrary code execution
- Externally Controlled String Violation: detect unsafe use of the *printf* family, output vital data
- Out-of-Bound Array Index: detect out-of-bounds writes/reads
- **Double Free:** detect repeat frees
- NULL Pointer Dereference: detect NULL dereferences, unintended memory access
- Use After Free: detect the illegal reuse of freed memory
- Weak Pointers: manipulate pointers, detect memory vulnerabilities
- Cryptographic Issues: encryption schemes, embedded keys, entropy
- **18,000 CVEs**: focused on known OT/ICS binary vulnerabilities
- ~140 CWEs: detected across 30 CPU architectures
- Dangerous Functions: detects over 100 dangerous functions
- Compliance Frameworks: incl. NIST 800 and ISA/IEC 62443
- Reports: Customizable reports
- **Delta**: Post-patch delta reports
- Integration: OpenAPI, SIEM

Who:

- Red Teams, Reverse Engineers, Threat Hunters, and Vulnerability Researchers Speed up your manual reverse engineering workflow. Dive deeper into binaries and firmware using advanced automated analyses that are too unwieldy, expensive, and slow to perform manually.
- DevSecOps Engineers, Product Security, QA Testers, and Software Developers

Detect vulnerabilities that source code analysis and SAST miss. Integrate into your DevSecOps pipeline via OpenAPI.

• Operators, Buyers/Procurement Reduce supply chain risks in your IT/OT/ICS environment. Require analysis in RFPs. Analyze during deployment and patching to ensure no vulnerabilities are introduced. Scan legacy devices to ensure they are safe, even if the manufacturer won't.



Scan to Visit Website



We provide precision vulnerability detection for defense and critical infrastructure.



815 E Street, Box #12070 San Diego, CA 92101 USA

Main US Phone: +1 (650) 515-3391

Email: salesinquiry@objectsecurity.com