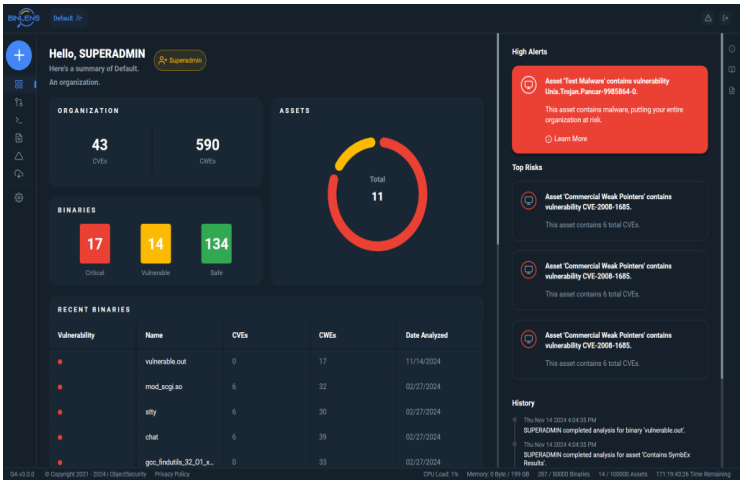
ObjectSecurity BinLens™
Automated Binary Vulnerability Analysis

ObjectSecurity™ BinLens™ 3.0

Automated Binary Vulnerability Analysis

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



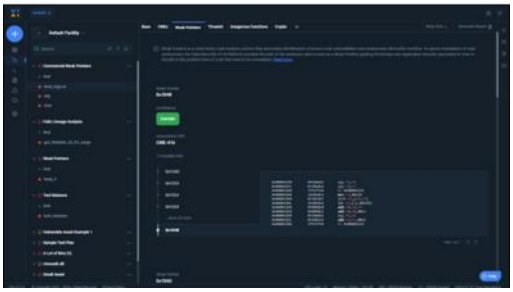
Why:

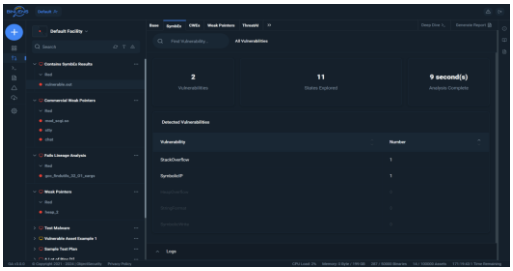
- SBOM generation is limited to detecting only known vulnerabilities in published software.
- Source code analysis and static application security testing (SAST) produce too many false-positives, slowing down remediation.
- Network scanning fails in cases where devices are not connected to the network.
- ~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.

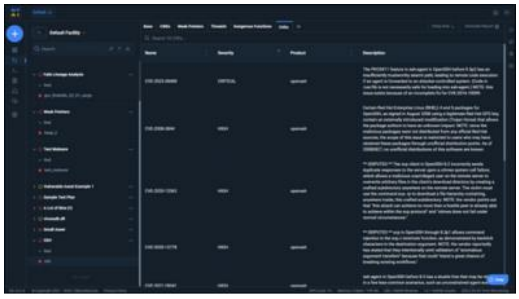
What:

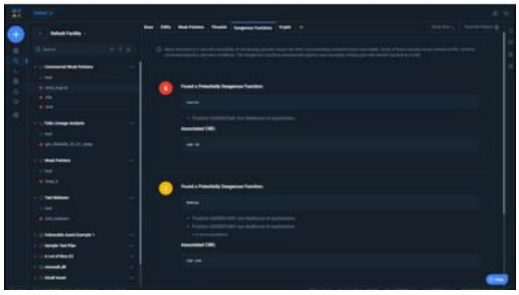
- Unlock deeper security insights with BinLens™ advanced binary analysis.
- Integrated approach combines multiple techniques to uncover potential zero-days with unmatched precision.
- Powered by automated symbolic execution, it excels at detecting memory-safety violations and other undefined behaviors 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™









Features:

- **Weak Pointers:** manipulate pointers, detect memory vulnerabilities
- **Stack Overflows:** detect unsafe writes to the stack frame
- **Heap Overflows:** detect unsafe writes to dynamically allocated memory
- **User Controlled Program Redirection:** detect user-controlled instruction pointers, arbitrary code execution
- **Externally Controlled String Violation:** detect unsafe use of the *printf* family, output vital program data
- **Out-of-Bound Array Index:** detect out-of-bounds writes, data corruption
- **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.

Request Quote

On-Prem, Offline VM

~or~

Secured VM in the Cloud

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

© Copyright 2022 - 2024 | ObjectSecurity, ObjectSecurity logo, BinLens, BinLens logo, OT.AI, OT.AI logo, ThreatAI are trademarks of ObjectSecurity LLC. All other trademarks, logos, and brand names are the property of their respective owners. All rights reserved.