SEI Bulletin

Trouble reading this email? View in browser.

Vessel Tool Enhances Container Reproducibility and Security

December 4, 2024—Software containerization has become an expected part of many DevSecOps software development and deployment pipelines. However, external dependencies during the container build process cause successive container builds to differ, decreasing trust in containers and possibly obscuring malware insertion. Vessel, an open source, first-of-its-kind tool recently released by the SEI, spots differences between successive container images and helps sort benign from problematic issues.

Containers suffer from the same reproducibility challenge as other software. Vessel reveals differences between container images and flags known issues, exposing potentially malicious tampering and dependencies on changing external resources. With this knowledge, developers can make their software more reproducible, stable, secure, and trustworthy.

Read more »

Get Vessel »

SEI News

Secure Software by Design 2024 Presentations Available
The presentations cover an array of ways to incorporate security earlier in the software lifecycle.

See more news »

Latest Blogs

Beyond Capable: Accuracy, Calibration, and Robustness in Large Language Models
For any organization seeking to responsibly harness the potential of large language models, we present a holistic approach to LLM evaluation that goes beyond accuracy.

Cyber-Physical Sensing to Extend the National Intelligence, Surveillance, and Reconnaissance Mesh
With the growing importance of improved sensing for national security, leveraging sensors in consumer products or embedded in devices can be economical, flexible, and timely.

See more blogs »

Latest Podcasts

Cybersecurity Metrics: Protecting Data and Understanding Threats
Scoping down objectives and determining what kinds of data to gather are persistent challenges in cybersecurity. Bill Nichols explores cyber metrics in our latest podcast.

3 Key Elements for Designing Secure Systems
To make secure software by design a reality, engineers must intentionally build security throughout the software development lifecycle. Timothy A. Chick discusses building, designing, and operating secure systems.

See more podcasts »

Latest Videos

Cyber Challenges in Health Care: Managing for Operational Resilience
Matthew Butkovic and Darrell Keeling explore approaches to maximize return on cybersecurity investment in the health-care context.

Independent Verification and Validation for Agile Projects
Justin Smith highlights a novel approach to providing independent verification and validation (IV&V) for projects that are using an Agile or iterative software development.

See more videos »

Latest Publications

Dangers of AI for Insider Risk Evaluation (DARE)
Austin Whisnant describes the challenges of using artificial intelligence for insider risk analysis and how to thoughtfully and efficiently use AI to find insider threats.

Assurance Evidence of Continuously Evolving Real-Time Systems (ASERT) Workshop 2024
This report summarizes the analysis of the Taiwanese flight CI202 incident as well as ideas for future work for ASERT presented at its 2024 workshop.

Secure Software by Design 2024 Presentations
SEI security researchers and industry software practitioners share ways to address, prevent, or eliminate security weaknesses earlier in the software development cycle.

See more publications »

Upcoming Events

FloCon 2025, March 4, 2025
FloCon is the SEI's annual conference on data-driven security.

See more events »

Upcoming Training

Software Architecture Design and Analysis
February 11-14, 2025 (SEI Live Online)

Insider Risk Management Measures of Effectiveness
February 19-21, 2025 (SEI Live Online)

See more courses »

Employment Opportunities

Reverse Engineer Researcher

Assistant Security Researcher

Special Programs Security Representative

All current opportunities »

Carnegie Mellon University
Software Engineering Institute