76 SWEG / SEI – Next Steps

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Carnegie Mellon University
Software Engineering Institute

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM21-0540

BLUF

SEI has been introduced to SWEG team work processes and environment. We have observed a talented and fast-moving team that has impressed us with their advanced technical capabilities. To better engage SWEG, given our current availability, we propose the following engagement:

Initial:

SEI, in collaboration with 76 SWEG, to write deployment hardening guidance, specifically to ensure secure configuration of Gitlab and ArgoCD in the planned deployment architecture

Forward-looking:

SWEG Reference Design for the complete picture of pipeline system design decisions and their impact on security, resilience and continuous authority to operation (cATO).

[[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

Background

Research has confirmed that attackers generally don’t exploit the software base (container). Most attacks are against vulnerabilities created by the configuration of the deployment. Pipeline administrators are faced with many complex and interdependent configuration choices that are critical to maintaining the security expected from hardened containers.

The DoD reference design provides initial guidance for implementers. However, different configuration and deployment choices will create cascading impacts that need to be understood in order to withstand cyber testing and remediate vulnerabilities discovered by those tests.

As an FFRDC, SEI has identified the value of tailoring reference designs for critical systems, from development to deployment, to enable efficient testing and accreditation.

Initial: Deployment Hardening Guidance 1

We propose specific deployment hardening, based on SWEG's use-case.

Initial analysis of current deployment of SWEG configurations of Gitlab (future iterations could cover ArgoCD and others) for the current/planned deployment architecture:

- Potential vulnerability surfaces
- Recommendations for a more robust pipeline deployment

This analysis would provide an initial resilience architecture plan to evaluate deployment tradeoffs and complexity for a portion of the deployment pipeline, tailored to the needs of SWEG.

Deliverables:

- Analysis report/evidence/guidance to support cATO process
- Actionable hardening deployment guidance

Initial: Deployment Hardening Guidance 2

An example analysis thread:

GitLab configuration behavior: Kicking off a GitLab build deploys Runners, conducts build processes, and runs through test steps.

Potential Vulnerability: The Runner is a point in the architecture, at which you absorb a fair amount of risk (arbitrary code introduced from anywhere, running and building it).

Recommendations: Security components such as GitLab Agent (client/server) should be architected to protect the main cluster from exposure to a compromised runner. Plan to manage the security sensitivity around that group of systems and how they are set up/torn down/isolated.

Analysis activities will include:

- Review of deployment and configuration documentation
- Interviews with SWEG teams to understand goals/needs

Initial: Deployment Hardening Guidance 3

Impact of Research:

DSO pipelines introduce systems complexity. Analysis is required to anticipate implications of configuration decisions to pipeline products/services. Combining enterprise products in arbitrary combinations introduces complex and subtle vectors of vulnerability for a system that needs to be resilient and verifiably secure.

Recommendations will address:

- Policy and architectural considerations that might show up in late-stage pen-testing and, if testing activity is successful, provide targeted remediation approaches for required rework.
- Both hardened deployment and improved Mean Time to Recovery, stopping intrusions and minimizing risks to the system if it is compromised.
- Provide evidence of architectural considerations for cATO

Forward-Looking: SWEG Reference Design [1]

This research project will build upon the Deployment Hardening Guidance to analyze the full deployment and provide insights required to achieve continuous ATO. Analysis will leverage USAF CTO guidance and focus on the unique configuration aspects of the SWEG pipeline.

Potential Deliverables:

- SWEG Reference design: Document articulating the security implications of software configurations and processes, how it differs from DoD references design, and how the current design contributes to the end goal of early system test integration
- White paper analysis study tying policy guidance to the pipeline data that they produce, and that configuration will help to achieve cATO objectives
  - What data SWEG will be required to provide
  - Concerns for their specific deployment

- Actual Infrastructure as code, implementing a Proof of concept with how system can provide the data required for cATO.

Forward-Looking: SWEG Reference Design 2

Impact of Research:

Creating a SWEG Reference Design will provide early insight into steps toward cATO for a unique pipeline deployment. (impact for all of DoD)

The Reference Design will be informed by SEI IA policy and DevSecOps expertise, providing insights to SWEG that begin to lower risk profile of major, late changes to system at certification.

The Reference Design will provide an artifact that facilitates clear communication with contractors and other pipeline stakeholders.