FEDRAMP VULNERABILITY SCANNING REQUIREMENTS FOR CONTAINERS

Version 1.0

3/16/2021

GSA

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
3/2021	1.0	All	Initial Publication	FedRAMP PMO

TABLE OF CONTENTS

1. Purpose

FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and Continuous Monitoring (ConMon) for cloud products and services. ConMon ensures CSPs continuously maintain the security of their FedRAMP Authorized systems by providing the Joint Authorization Board (JAB) and Agency Authorizing Officials (AOs) insight into the security posture of the system over time. Technology changes rapidly, and CSPs continue to evolve in order to improve and adapt to customer needs. Some technology changes affect how ConMon is performed. This document addresses FedRAMP compliance pertaining to the processes, architecture, and security considerations specific to vulnerability scanning for cloud systems using container technology.

2. Background

The *FedRAMP Vulnerability Scanning Requirements for Containers* bridges the vulnerability scanning compliance gaps between traditional cloud systems and containerized cloud systems.

The requirements described in this document are part of the *FedRAMP Continuous Monitoring Strategy Guide* and *FedRAMP Vulnerability Scanning Requirements*. The vulnerability scanning requirements for containerized systems serve to supplement and update existing requirements defined in those documents.

Container technology can be deployed on bare metal or virtual machines, on-premise systems, or within elastic cloud environments. Various container orchestration tools are typically used to enable deployment and management of distributed containers at scale. Some of most common characteristics of container technology are[1]:

- Containers run application(s) and their dependencies that should be isolated from other processes
- Containers have network connections that are host independent
- Containers are elastic and sometimes ephemeral in nature
- Containers are immutable, upgrades occur on a source image in a secure staging environment and upgrading a container involves destroying an existing container and replacing it with a new container

Important risks and threats relative to the use of containerization technology include:

- Unvalidated external software
- Non-standard configurations

[1] The characteristics, risks, and terms contained in this document are derived from the *NIST SP 800-190, Application Container Security Guide* (published September 2017), and industry input.

- Unmonitored container-to-container communication
- Ephemeral instances that are not tracked
- Unauthorized access
- Registry/repository poisoning
- Unmanaged registry/repository

The security requirements listed within this document facilitate a CSP's ability to leverage container technology while maintaining compliance with FedRAMP. The intent of the following security requirements are to ensure that risks relative to the use of container technology are mitigated or otherwise addressed (including but not limited to those listed in bullet-point form above). The requirements apply broadly and FedRAMP recognizes that certain implementations may call for alternative measures to address risk.

3. Scanning Requirements for Systems Using Container Technology

Existing scanning requirements are outlined in the *FedRAMP Continuous Monitoring Strategy Guide*, the *FedRAMP Low, Moderate, and High Security Control Baselines*, and the *FedRAMP Vulnerability Scanning Requirements* documents.

The following requirements are supplemental and are applicable for all systems implementing container technologies:

- **Hardened Images:** The CSP must only utilize containers where the image is "hardened." Where applicable, the hardening must be in accordance with relevant benchmarks listed in the National Checklist Program and defined by the National Institute of Standards and Technology (NIST) SP 800-70. Benchmarks are used as a baseline and may be altered. However, the final configurations must be validated by a 3PAO to ensure they meet FedRAMP requirements for the baseline controls CM-6, SC-2, SC-3, SC-4, SC-6, SC-28, and SC-39. In the case of containers leveraging an image that does not have a listed benchmark available, the CSP must create and maintain a 3PAO validated benchmark for the purpose of hardening. Non-hardened or general-purpose images may not be used within the authorization boundary. The 3PAO must validate the CSP process of hardening images intended for deployment. 3PAO validation of every individual container instance deployed to production is not required. This requirement does not restrict a CSP from leveraging third-party software within hardened containers. This requirement also does not restrict a CSP from using hardened images or software obtained from a secure repository in groups which share IP addresses and may share volumes.

- **Container Build, Test, and Orchestration Pipeline:** The CSP must leverage automated container orchestration tools to build, test, and deploy containers to production. These automated tools must

be validated by a 3PAO to meet FedRAMP requirements for the baseline controls CA-2, CM-2, CM-3, SC-28, SI-3, and SI-7. However, components of the pipeline that fall to the left of the production container registry, including environments intended for development or testing, may reside outside of the system boundary. Non-automated processes should not be considered part of the container testing and orchestration process, except in the case of intentional manual procedures for quality review purposes. These processes and tools must include a mechanism to restrict containers that do not adhere to FedRAMP requirements from successfully deploying.

- **Vulnerability Scanning for Container Images:** Prior to deploying containers to production, a CSP must ensure that all components of the container image are scanned as outlined in the *FedRAMP Vulnerability Scanning Requirements* document. When possible, the container orchestration process should incorporate scanning as one of the steps in the deployment pipeline. The 30-day scanning window begins as soon as the container is deployed to the production registry. Only containers from images that have been scanned within a 30-day vulnerability scanning window can be actively deployed on the production environment. Additionally, modification of configuration settings defined within the image or software patching should never occur directly on the production environment, but rather on the replacement image to be deployed to production. Performing vulnerability scanning directly on containers deployed to production is not recommended, unless it is performed via the use of independent security sensors deployed alongside production-deployed containers.

- **Security Sensors:** Independent security sensors may be deployed alongside production-deployed containers to continuously inventory and assess a CSP's security posture. This independent deployment allows the security sensors to maintain broad visibility across containers. Security sensors should be run with sufficient privileges to avoid lack of visibility and false negatives. If utilized, security sensors should be deployed everywhere containers execute to include within registries, as general-purpose sensors, and within CI/CD pipelines. If this approach is taken, the sampling guidance found in the *Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans* document may be applicable.

- **Registry Monitoring:** The container registry must be monitored per unique image to ensure that containers corresponding to an image that has not been scanned within the 30-day vulnerability scanning window are not actively deployed on production. As the registry itself is often not a policy control point, this process may be managed by alarms that inform operators or other control mechanisms to prevent unauthorized deployment.

- **Asset Management and Inventory Reporting for Deployed Containers:** A unique asset identifier must be assigned to every class of image which corresponds to one or more production-deployed containers. These image-based asset identifiers must be documented in the *FedRAMP Integrated Inventory Workbook Template*. Instances of production-deployed containers must be tracked

internally by the CSP via an automated mechanism, which must be validated by a 3PAO to meet the baseline control CM-8. Every production-deployed container must correspond to the image from which the deployed container originated, in order to identify the total number of relevant vulnerabilities on production associated with that container. While individually deployed instances of containers should be tracked internally by the CSP, they do not need to be included as part of the *FedRAMP Integrated Inventory Workbook Template*, unless they are specifically the target of a scan performed by a security sensor. If they are the target of a scan performed by a security sensor, they must be included as part of the *FedRAMP Integrated Inventory Workbook Template* ConMon deliverable, in accordance with the *Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans* document, if applicable.

4. Transition Plan

If applicable, each FedRAMP system leveraging container technology has 1 month to provide a transition plan and 6 months from the release date of this document to transition into full compliance.

Where full implementation is not possible, the CSP must work with their AO on a mitigation plan. The AO must review and approve the CSP's mitigation plan. For systems with a JAB P-ATO, the CSP should post the mitigation plan to the FedRAMP repository and send an email notification to info@fedramp.gov, or discuss an alternative arrangement with their FedRAMP POC. Any CSPs currently authorized by Agency AOs will need to consult with their AO.