FedRAMP® Vulnerability Scanning Requirements

Version 2.0

02/15/2024

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
03/20/2018	1.0	All	Initial document that replaces FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide	FedRAMP PMO
07/14/2022	2.0	All	Added in Container guidance and updated language throughout	FedRAMP PMO
02/15/2024	3.0	All	Consolidated all required scanning requirements. Added and refined language for container scanning, encryption and reporting. Clarified supplemental scanning remediation reporting.	FedRAMP PMO

ABOUT THIS DOCUMENT

This document has been developed to provide guidance on vulnerability scanning policy, procedures, and tools in support of achieving and maintaining a security authorization that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements.

Some cloud service providers (CSPs) may need to transition from their current vulnerability scanners or work with their vendors in order to meet the requirements.

This document is not a FedRAMP template – there is nothing to fill out in this document.

This document uses the term authorizing official (AO). For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says agency AO. For systems with a FedRAMP Agency Authorization to Operate (ATO), AO refers to each leveraging agency's AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by CSPs, third party assessment organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP projects.

How to Contact Us

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

1.0 Purpose

Continuous monitoring (ConMon) ensures CSPs continuously maintain the security of their FedRAMP Authorized systems by providing the Joint Authorization Board (JAB) and authorizing officials (AOs) monthly insight into the security posture of the system. CSP scanning policies, procedures, and tools (including vulnerability scanners) are key components to ConMon activities. In an effort to increase the efficiency and effectiveness of ConMon activities, the FedRAMP Program Management Office (PMO) provides guidance for scanning requirements. This document summarizes those requirements.

2.0 Background

The vulnerability scanning requirements are part of the FedRAMP Continuous Monitoring Strategy Guide and the appropriate FedRAMP Low, Moderate, or High security control baselines, specifically in control RA-5.

The ConMon scanning requirements move FedRAMP ConMon activities toward efficiencies, advance the quality of ConMon information provided to FedRAMP, and better position FedRAMP to perform robust analysis in the near future. These changes also better enable FedRAMP to scale up as the volume of FedRAMP Authorized systems continues to increase.

Further, FedRAMP has an obligation to determine and enforce CSP compliance with such security requirements.

3.0 Scanning Requirements

Scanning requirements are also outlined in the FedRAMP Continuous Monitoring Strategy Guide and the FedRAMP Low, Moderate, and High security control baselines.

This document expands on the original requirements:

- **Scanner Resiliency:** Scanners should be hardened to resist unauthorized use or modification (i.e., unnecessary ports and/or unnecessary services should be closed).
- **Authenticated Scanning:** For Moderate and High systems, the CSP must ensure authenticated scans are performed wherever possible. [RA-5(5)]
- **Scanning with Full Authorization:** For all Moderate and High systems, the CSP must ensure that scans are being performed with full system authorization. [RA-5(5)]

    - Scanning must avoid typical lack of authorization issues (including lack of access to remote registry, limited registry access, limited file access, etc.).
- **Machine-Readable Findings:** The scan output must display all scan findings with a low risk or higher in a structured, machine-readable format (such as XML, CSV, or JSON).
    - If the scanner is able to output/export findings in more than one machine-readable format, the CSP must select the format that provides the greatest amount of information.
    - Where possible, the machine-readable data must include the authentication and authorization status of the scans to demonstrate the degree to which an authenticated scan was performed on each host.
- **National Vulnerability Database (NVD):** For any vulnerability listed in the latest version of the National Institute of Standards and Technology (NIST) NVD, the Common Vulnerabilities and Exposures (CVE) reference number must be included with the machine-readable findings data for that vulnerability.
- **Common Vulnerability Scoring System (CVSS) Risk Scoring:** For any vulnerability with a CVSSv3 base score assigned in the latest version of the NVD, the CVSSv3 base score must be used as the original risk rating. If no CVSSv3 score is available, a CVSSv2 base score is acceptable where available. If no CVSS score is available, the native scanner base risk score can be used.
- **Configuration Settings:** The CSP must provide machine-readable evidence that the scanner's configuration settings have not been altered from the 3PAO-validated configuration settings approved during the initial authorization assessment.
- **Configuration Changes:** If a scanner configuration change is required (above and beyond normal patching and updates) the AO must be notified and approve of the change.
- **Signature Updates:** For each deliverable, the CSP must update the list of vulnerabilities scanned to the latest available list. [RA-5(2)]
    - The CSP must use a vulnerability scanner that checks for automatic signature updates of the scanner's vulnerability database at least monthly.
    - The CSP must provide automated machine-readable evidence of the most recent update performed prior to scanning.
- **Adequate Asset Identification:** The scanner findings must contain unique asset identifiers that map to an inventory.
    - The CSP must have an automated mechanism to identify and catalog all assets, within the authorization boundary, every month in order to ensure that everything is being scanned appropriately
    - For Web scans, a dynamically updated catalog of Web services should be maintained to include the ports where Web services reside.
- **Types of Scans:** CSPs must scan operating systems, Web applications, and databases monthly. All scan reports must be sent to the AO/JAB monthly. [RA-5]
    - The entire inventory (or approved sampling percentage) within the boundary must be scanned at the operating system (OS) level at least once a month.

  - All Web interfaces and services (or approved sampling percentage) must be scanned.
  - All databases (or approved sampling percentage) must be scanned, including those required to support the infrastructure.
- **Plan of Action and Milestones (POA&M) Entries:** The CSP must track each unique vulnerability as an individual POA&M item.
  - Individual vulnerabilities must be based on the scanning tool's unique vulnerability reference identifier (ID).
  - The CSP may break a unique vulnerability into multiple POA&M items, such as for a vulnerability that applies to different asset types that will be remediated in different ways.
  - The CSP must not group multiple unique vulnerabilities into a single POA&M item.
- **All Non-Destructive Detections:** The CSP must enable all non-destructive detections within the scanner.
- **Image Scanning:** Where the CSP offers services, such as virtual images, and where the customer is responsible for scanning but is reliant on the CSP for patching, the CSP must scan the source image for all available customer leveraged images.
  - This applies to all images in use or available for use by federal government customers.

4.0 Scanning Requirements for Systems Using Container Technology

The below vulnerability scanning requirements are specific to and for use with containerized systems. This guidance serves to supplement the requirements defined elsewhere in this document as well as guidance found within the FedRAMP Low, Moderate, and High Security Control Baselines and FedRAMP Continuous Monitoring Strategy Guide.

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.

[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.

- 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
- 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.

- **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. Any hardened image put into production should not contain vulnerabilities previously identified by CISA in the Known Exploited Vulnerability Catalog.
- **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. This should be accomplished in the development environment by a scanner that meets this document's guidelines for this process and those scans provided to the AO or JAB as part of the monthly ConMon submission. 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.
- **Encryption:** FedRAMP considers any data in transit, whether that be from one container to another container, from a container to a sidecar inside the same host virtual machine, or from a container to

any other source outside that container, that SC-8 controls must be applied to this data in transit. SC-8 protection (usually encryption) is required when data is in transit from one memory processing space to another.

These requirements ensure AOs are able to provide high-quality ConMon oversight across a CSP's system and ensure consistency in scan results for AOs to analyze across multiple systems.

Only scanning tools that meet the revised requirements will be accepted by FedRAMP for ConMon. This may impact the current ConMon strategy of some CSPs. The FedRAMP PMO can assist CSPs to determine if other scanners are able to meet FedRAMP requirements.

> **Note:** CSPs and 3PAOs must ensure that all scan results obtained for a specific assessment/point in time (remediation scan) MUST be in the same format (by scan type and scanner type) (e.g., all fields covered in the original scans must be accounted for in the remediation scans). If the scan results do not align, this can/will prolong the FedRAMP authorization due to the need for the 3PAO or CSP to reconcile scan results.

Appendix A: Glossary

Asset: A physical or virtual device or component within an information technology system, identified by a unique asset ID.

Authentication: A scanning tool's ability to log in with administrative privileges on an asset in order to perform a scan with elevated privileges.

Authorization: A scanning tool's ability to access the registry and files on an asset remotely in order to perform a full scan.

Detection: An individual program within the scanning tool that checks for a given vulnerability or other data point (authentication, etc.) that is flagged as a finding, identified by a unique detection ID.

Vulnerability: A scan detection that relates to a specific weakness, identified by a unique vulnerability ID.