STATERAMP VULNERABILITY SCAN REQUIREMENTS GUIDE

VERSION:
1.0
DATE:
August 2022

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

Date	Description	Version	Governance Body
7/22/2022	Policy Approved	1.0	Standards & Technical Committee
8/7/2022	Policy Adopted	1.0	Board of Directors

This document will be reviewed at the discretion of the StateRAMP Board at a frequency of no less than annually.

WHO SHOULD USE THIS DOCUMENT

This document is intended for the use by the following groups:

1. StateRAMP service providers (SP) to ensure they provide vulnerability scans as required.
2. StateRAMP PMO, to ensure the requirements are met and maintained.
3. Leveraging state, local, and higher education (SLED) to understand the scanning required by SPs.

For more information about StateRAMP, visit the website at www.stateramp.org.

1. PURPOSE

This guide describes the requirements for all vulnerability scans provided by service providers to StateRAMP for products with a Ready, Provisional, or Authorized status.

2. SERVICE PROVIDER REQUIREMENTS

Service providers are required to perform vulnerability scanning of their information systems monthly (at a minimum). Each SP is responsible for the delivery of the results of these vulnerability scans to the StateRAMP PMO in a timely manner. These vulnerability scans are the cornerstone for the continuous monitoring of a SP's risk posture, enabling the StateRAMP PMO and the StateRAMP Approvals Committee (SAC) or the state, local, or higher-education (SLED) entity's Authorizing Official (AO) to determine the technical security posture of the system.

Each SP must identify and use vulnerability assessment tools within their security control implementations. These include:

- Operating system and network vulnerability scanners
- Database vulnerability scanners
- Web application vulnerability scanners

StateRAMP security authorization requirements specify that initial vulnerability scans shall be performed by a Third Party Assessment Organization (3PAO), to provide independent validation of the scan results.

To ensure the StateRAMP PMO has all the required information to perform the vulnerability analysis, the SP must submit the following information:

1. Vulnerability scan data
    a. Raw scan files in CSV or Excel format.
    b. Exported summary reports (PDF, MS Word, or other readable documents).
    c. Summary reports should include Executive Summary, Detailed Summary, and Inventory Report. Actual reporting capabilities may vary by tool.
2. Current and accurate system inventory, and to include:
    a. System inventory identifying the components of the information system within the authorization boundary.
    b. The inventory must be complete and contain all boundary components.
    c. The inventory must be in the StateRAMP template unless the system has gone through the FastTrack process, in which case the FedRAMP template will be accepted.
3. It is critical that the vulnerability scans and the provided system inventory is machine readable (IP addresses, system names, or other unique identifiers). Vulnerability scans and inventories that cannot be matched will by rejected by the PMO.

Below is a list of requirements to ensure the quality of the scanning is acceptable for the StateRAMP program.

4. **Authenticated/Credentialed Scans:** Vulnerability scans must be performed using system credentials that allow full access to the systems. Scanners must have the ability to perform in-depth vulnerability scanning of all systems (where applicable). Systems scanned without credentials provide limited or no results of the risks. All unauthenticated scans will be rejected unless an exception has been previously granted due to applicability or technical considerations.
5. **Enable All Plug-ins:** To ensure all vulnerabilities are discovered, the scanner must be configured to scan for all findings.
6. **Full System Boundary Scanning:** Each scan must include all components within the system boundary.
7. **Scanner Signatures Up to Date**: SPs must ensure that the vulnerability scanner used is up to date and includes the latest versions of the vulnerability signatures. Before scanning, each scanner must be updated to reflect the latest version of the scan engine as well as the signature files.
8. **All Findings Must Be Added to the Monthly POA&M**: Findings within the scans must be addressed in a Plan of Action and Milestones (POA&M) as described in the POA&M Template User Guide on StateRAMP website www.stateramp.org

3. REMEDIATION

Systems that fail to meet the quality or timeliness of the vulnerability scan submission requirements will be subject to remedial actions which may include one or more of the following:

- The StateRAMP PMO may require an immediate re-scan of the system. The PMO will clearly document the required adjustments necessary for the re-scan.
- The StateRAMP PMO may require a 3PAO to perform future scans for a period of time if the SP is unable to meet the StateRAMP requirements.
- Continuous issues may result in the StateRAMP PMO requiring a Corrective Action Plan from a SP as part of maintaining any one of the verified statuses and communicating the deficiencies with meeting scanning requirements with the SAC or the AO.
- The StateRAMP PMO can revoke a Ready status for failure to meet these requirements. The StateRAMP PMO, the StateRAMP Approvals Committee (SAC) or the State, local or higher education (SLED) entity's Authorizing Official (AO) can revoke a Provisional or Authorized status for failure to meet these requirements. In such cases, the service offering will be removed from the Authorized Vendor List (AVL). StateRAMP and the StateRAMP PMO reserves the right to take any of the actions listed above based on the severity of the deficiency.