tenable.io

QUICK SHEET

Remediation Scans

OVERVIEW

This document describes remediation scans in Tenable.io and how to use them to ensure critical vulnerabilities have been remediated.

LAUNCHING A REMEDIATION SCAN IN TENABLE.IO

1. To launch a remediation scan, you must have the following user role and access group permissions:
    a. Roles: Scan Operator, Standard, Scan Manager or Administrator
    b. Access Group Permissions: Can Scan
2. Remediation scans on scan results can only be performed from using Tenable connected Nessus scanners.
3. To launch a remediation scan, follow the steps outlined in Launch a Remediation Scan in the Tenable.io User Guide.

REMEDIATION SCAN TIPS

1. You can easily launch a remediation scan directly on the Vulnerability Details page or the Asset Details page using the Actions button on the top right of the page.
2. Use caution when running a remediation scan for a plugin that requires scan credentials. If you neglect to add scan credentials when required for a specific plugin, or if you type the credentials incorrectly, the system will not have sufficient access to detect if the vulnerability is fixed. This is because vulnerabilities can not change state if not detected by the same Authentication level.
3. Tenable.io assigns a vulnerability state (new, active, fixed, resurfaced) to all vulnerabilities on your network. You can track and filter by vulnerability state to see the detection, resolution, and reappearance of vulnerabilities over time.
4. You can create an asset filter to view and report on assets where a vulnerability was recently mitigated.
5. Use the Mitigation Summary dashboard in Tenable.io to track vulnerabilities as they are fixed, get a summary of outstanding vulnerabilities, and view current and mitigated vulnerabilities.
6. You can automate remediation scans using the API.

WHAT IS A REMEDIATION SCAN?

A remediation scan evaluates a specific plugin against a specific scan target or targets where a vulnerability was discovered in earlier active scans.

REMEDIATION SCAN BENEFITS

- Quickly target specific vulnerabilities that previous scans identified on your assets.
- Validate remediation of the vulnerabilities identified in previous scans.
- Helpful during remediation testing cycles, as scans are completed more quickly than regular, active scans. This is especially useful for a user or team that is responsible for remediating only certain sets of vulnerabilities.

ADDITIONAL RESOURCES

Tenable.io User Guide: Launch a Remediation Scan

Tenable.io Scanning Best Practices

tenable