Tenable Vulnerability Management Update (formerly Tenable.IO) in FedRAMP Moderate

Targeted for General Availability the week of **April 8, 2024**

This document describes feature and functionality updates to Tenable Vulnerability Management (VM) in the FedRAMP Moderate environment. It is for all FedRAMP customers.

Table of Contents

API

For information about changes to the API, see the Changelog on the Tenable Developer Portal. Changes later than October 2021 apply to this update.

Dashboard Templates and Widgets

- You can now identify, review, and update your dashboards and widgets with the latest dashboard templates and widgets from Tenable Vulnerability Management.

Other Enhancements

- Tenable Vulnerability Management has a new integration with Microsoft Azure Sentinel.
  For more information, see Microsoft Azure Sentinel in the *Tenable and Microsoft Azure Integration Guide*.
- Tenable Web App Scanning now supports the OWASP Top 10 2021.
  For more information, see the OWASP Top 10 website.
- Tenable Web App Scanning now supports these data sources when reviewing plugin details: OWASP ASVS, NIST, HIPAA, PCI DSS, ISO, CAPEC, and DISA STIG.
  For more information about the new data sources, see Tenable Plugins.
- You can now use API Key and Bearer Token credentials in Tenable Web App Scanning scans.

Log4shell dashboard and scan templates

- There is a new **log4shell Critical Vulnerability** dashboard template.
  For more information and a list of widgets, see log4shell Critical Vulnerability.
- There are three new scan templates to detect the log4shell critical vulnerability in your network:
  - Log4Shell
  - Log4Shell Remote Checks
  - Log4Shell Vulnerability Ecosystem

Rule-based Agent Scanning and Agent Updates

- Rule-based Agent Scanning - You can now configure Agent scans with scan triggers. With scan triggers, an Agent initiates scans based on a specified time interval or file name.
  For more information and a list of widgets, see Basic Settings in Vulnerability Management Scans in the *Tenable Vulnerability Management User Guide*.
- Agents will now update Tenable Vulnerability Management with their host asset information any time a change is detected, regardless of the last scan completion, providing you with a more up-to-date understanding of your asset configuration.
  The host metadata includes:
  - MAC addresses
  - All IPv4 and IPv6 addresses
  - Version information (e.g., engine, plugin set)
  - Nessus Agent platfrom
  - EC2 instance metadata
  - Hostname, if configured
  - Host OS information

Dashboards and Widgets

- There are three new dashboards in Tenable Vulnerability Management:
  - 2021 Threat Landscape Retrospective
  - Asset Inventory and Detection (SEE)
  - Defending Against Ransomware (ACT)
- There are updates to three Tenable Vulnerability Management widgets:
  - *BOD 22-01 - DHS Tracked Known Exploited Vulnerabilities* - Added a **Fixed** column and new rows for due dates.
  - *log4shell - Log4j Concerns* - Added a **Fixed** column.
  - *Vulnerability Overview by CVE* - Added a new row for 2021 - 2025.

Other Enhancements

- You can now create dashboard groups and share them, instead of sharing dashboards one at a time.
- The **Solutions** and **Scan Templates** pages in the **Vulnerability Management** section have a new data list view that allows users to select, resize, and reorder columns with improved pagination and user actions.
  For more information, see Interact with a Customizable Table in the *Tenable Vulnerability Management User Guide*.

Custom Certificates

You can now upload custom certificates to scan policies using the Advanced Network Scan template.

For more information, see Advanced Settings in Vulnerability Management Scans in the *Tenable Vulnerability Management User Guide*.

Report Scheduling

Report scheduling: You can now configure reports to run on a customizable schedule.

Explorer Workbenches, Tagging, Export, and RBAC

- New pages in the **Analysis** section:
  - **Explore** page: Diagnose, analyze and visualize program trends with a customizable dashboard. You can see asset and vulnerability trends over time, and customize trends by time interval, scan duration, and more.
  - **Findings** page: A single view for all Tenable Vulnerability Management and Tenable Web App Scanning vulnerabilities, audits, and misconfigurations.
  - **Assets** page: A single view for all Tenable Vulnerability Management and Tenable Web App Scanning assets.
  - **Reports** page: Create, schedule, and run reports and view your report results.
- Filtering enhancements:

    - **Universal Filter Component:** One common set of filters used across the platform to simplify filtering.
    - **Multi-dimensional Filtering:** You can use multiple filters simultaneously.
    - **Advanced filtering:** You can filter using and/or stipulations, wild card placeholders, and exists/does not exists values.
- Tagging enhancements:
    - **Asset management:** Tags are now the primary way to organize, group and control access to assets.
    - **Target groups not needed:** Tags can be used for discovery scans, eliminating the need for target groups.
    - **Tag management:** There is a more intuitive tag management process with consistent behavior across Tenable Vulnerability Management.
    - You can create and use tags to build a list of targets to scan without the need to configure separate target groups.
- Export enhancements:
    - **Export consistency:** The export experience is now integrated throughout Tenable Vulnerability Management.
    - **Dashboard exporting:** Nearly all data sets on the platform can be exporting, including: asset data, vulnerability data, user data, scanner and agent management data and even export data.
- Role-based access control (RBAC) enhancements:
    - **Centralized access control:** You can manage roles, users, groups and permissions from one central location.
    - **Custom user roles:** Administrators can now create custom user roles.
- Scan enhancements:
    - You now have the ability to pause or resume a scan.

Self-service Security Settings

- Multi-factor authentication: Self-service security settings are now available to Administrators in Tenable Vulnerability Management. With these security settings, users with Administrator privileges can:
    - Allow users on their organization's instance to generate API keys.
    - Require users on the instance to set up multi-factor authentication.
    - Allow users on the instance to log in to their accounts using a SAML single sign-on (SSO).

    - Allow users to log in to their accounts using a password.

Scanning UI Updates

- Renamed the **Scanner** and **Agent** Vulnerability Management scan template categories to **Nessus Scanner** and **Nessus Agent**, respectively.
- Updated the scan **User Permission** role names for more clarity.
- Added a **Scanner** dropdown to the Nessus Scanner > **Basic Settings** page that allows you to choose between cloud or internal/local scanners.
- You can now edit scanner sensor names.
- Added two Nessus Agent settings: **offline_agent_scan_trigger_execution_threshold_days** and **maximum_scans_per_day**.
- Added tooltips to pages and fields related to **Tags**, **Networks**, and scanner selection.

Advanced Query Updates

- When you make an advanced query while creating a tag rule or filtering assets, you can now use the tag name in addition to the UUID.
- When you make a typo in an advanced query, an error will appear with a description of the issue.

Tagging Improvements

- You can now add up to 10 tags in **Basic** mode, and choose whether Tenable Vulnerability Management uses *AND* or *OR* logic for certain tag rules when applying tags.
- In **Basic** mode, instead of tag UUID values, Tenable Vulnerability Management displays tag category and value names when a tag rule uses an existing tag as part of the rule.

Export Permission Configurations

You can now export your access control permission configuration data in CSV and JSON format.

Scan Settings Updates

- **Scan Window**: Added a new **Scan Window** setting that allows you to identify a time limit for your Vulnerability Management Nessus scan configuration. When scans reach the end of the scan window, they will complete the current plugin being executed before halting. All successfully scanned asset findings will be available in Tenable Vulnerability Management.
- **Scanner Type**: Added a **Scanner Type** drop-down that allows you to choose between cloud and internal/local scanners when configuring Tenable Web App Scanning scans. This allows you to more easily identify the scanner needed for your scan configuration.

Export Roles

You can now export your roles in CSV and JSON format.

Export Groups

You can now export your user group data in CSV and JSON format.

Export Freeze Windows

You can now export your freeze window data in CSV and JSON format.

Scheduled Exports in Tenable Vulnerability Management

Administrators can now schedule export jobs to occur on a repeating schedule. Administrators can also view, enable, disable, or delete scheduled exports from the **Exports** page.

All Tags Access for Permissions

Administrators can now use the All Tags feature to give users *Can Edit* and *Can Use* permissions for all object tags on their account.

RBAC Permissions for Tags

Administrators can now grant users Can Edit and Can User permissions to Tags.

Findings Exports

Networks and Tags are now available in Findings Exports.

Advanced Filtering

There is a new advanced filtering component in Assets, Findings, and Tags with additional filters and operators.

Custom Role with View-Only Privileges for Assets and Findings

The custom role functionality in Tenable Vulnerability Management now includes the ability to create a role with view-only privileges for your Explore assets and findings.

Grouping for Host Vulnerabilities Findings

You can now group your host vulnerability findings by asset name or plugin ID in Tenable Vulnerability Management.

Rename Linked Scanners and Agents

You can now rename linked scanners and agents from the Tenable Vulnerability Management user interface.

Unified Scan Configuration

Tenable Vulnerability Management and Tenable Web App Scanning scanning configuration is now unified in one location to simplify scan management in Tenable Vulnerability

Management. The new view is available via the **Scans** menu item in Tenable Vulnerability Management, and contains tabs for Tenable Vulnerability Management and Tenable Web App Scanning scans.

Web Application and Nessus Findings Filter Parity with Vulnerability Filters

The Nessus and Web Application vulnerability findings filters are now consistent with the filters in the Vulnerabilities workbench. The filters are available in the Host Vulnerabilities and Web Application Vulnerabilities tabs on the **Findings** page in the **Explore** section of Tenable Vulnerability Management.

Remediation Projects and Goals

You can now create Remediation Projects and Remediation Goals to prioritize, distribute, and track vulnerability tasks in the environment.

Export Remediation Projects and Goals

You can now export your Remediation projects and goals data in CSV and JSON format.

Self-Service Conversion of Access Groups to Permission Configurations

Administrators can now convert one or more access groups on their accounts into permissions configurations. When you convert an access group to a permission configuration, the access group no longer appears on the **Access Groups** page and can be accessed only via the API. When you have converted all your access groups into permission configurations, the **Access Groups** page and tile no longer appear in the interface.

Kerberos Credential Authentication for Web Application Scans in Tenable Vulnerability Management

You can now use Kerberos Credential Authentication for your web application scans in Tenable Vulnerability Management.

Quick Scan Template for Tenable Web App Scanning

A new scan template called **Quick Scan** has been added to the list of Tenable Web App Scanning scan templates.

Grouping for Web Application Findings

You can now group your web application vulnerability findings by asset name or plugin ID in Tenable Vulnerability Management.

Search and Filter Scheduled Exports in Tenable Vulnerability Management

Tenable has added the ability for users to search for and filter scheduled exports in Tenable Vulnerability Management. Users can now search for specific schedules in the search bar and set filters in the filter panel to display only their desired scheduled exports.

Rollover Scans in Tenable Vulnerability Management

You can now launch rollover scans for Tenable Vulnerability Management scans that did not previously finish due to timing out. Rollover scans allow you to achieve complete scan coverage for all your assets, and you can use the rollover feature to split up large, network-impacting scans. You can also download a list of a scan's remaining rollover targets from the **Scan Details** page.

For more information, see Launch a Rollover Scan and Download a Rollover Target List in the *Tenable Vulnerability Management User Guide*.

Risk Modified Filter

"Risk Modified not equal to Accepted" is now a default filter in the Vulnerabilities tab in Tenable Vulnerability Management and Tenable Web App Scanning. This filter indicates whether you have accepted or recasted (or both) the severity of a vulnerability.

Applied Filters Limit increased to Nine

To optimize performance, Tenable Vulnerability Management has increased the number of filters that you can apply to any Explore > Findings or Assets views (including Group By tables) to nine.

Increased Plugin Output Details

Plugin output details are now available on the findings details preview pane and details page.

Plugin Output Data Retention Disabled by Default

You must enable the plugin output data retention option to use the Plugin Output filter and run a scan. Data retention does not start until after data retention is enabled.

New Privileges Available in Custom Roles

Administrators can now add privileges to a custom role that allow users to read or manage data in the following areas of Tenable Vulnerability Management:

- **Explore** > **Assets**
- **Explore** > **Findings**
- **Dashboards**
- **Accept/Recast**

Access Control Enhancement

When an Administrator creates a new user in Tenable Vulnerability Management, they can limit the user's access to either the Tenable Vulnerability Management interface or API.

Filter By and Filter Out Functionality for Assets and Findings Tables

By right-clicking on a cell within the table the user can filter by or filter out the value of that cell. This work is to allow quick filtering of the data the user sees within the table, enabling them to get directly to the day they want to see in the least number of clicks possible.

Filtering in Reports

You can now filter your reports by all assets, assets by tag, and custom assets.

Updated Pagination for Group By tables

You can paginate the group by table just like the search (list) table. There is no longer a 200 row limit.

Copy to Clipboard Functionality for Assets and Findings Tables

By right-clicking on a cell within an Assets or Findings table, you can copy to your clipboard the value of that cell.

Windows Host Data Normalization

Tenable has standardized Windows operating system (OS) name values that appear in the Tenable Vulnerability Management user interface. All Windows OS name values collected from credentialed scans now appear using the following format: *<vendor> <os> <version> <edition> <update>* (for example, "Microsoft Windows 11 Enterprise Build 22621").

Before this update, Windows OS name values would appear with minor variations based on whether Tenable Nessus scanners or Tenable Nessus Agents generated the data.

If you have built filters, saved searches, and tags that are filtered on expected variations of specific OS values (for example, *Microsoft Windows Server 2019 Datacenter 10.0.17763*), Tenable recommends updating these saved filters.

> **Note:** This update only applies to Windows OS data in the English user interface. Tenable plans to release similar updates for other languages and OS types in the future.

For more information, see the Tenable Windows Host Data Normalization FAQ.

Asset Tags on the Findings Workbench

Tenable has added new filters and columns to the **Findings** workbench. These additions enhance how you work with asset tags.

- With the **Asset Tags** filter, search the **Findings** workbench for vulnerabilities or host audits that contain the asset tags you specify.
- In the **Asset Tags** column on the **Findings** workbench, view all asset tags for a finding.

For more information, see Findings Filters.

Findings Filter Enhancements

Tenable has simplified the **Plugin Output** filter on the **Findings** workbench. This filter now uses operators instead of regular expressions.

For more information, see Findings Filters.

Relocate Open Port Findings

Tenable is pleased to announce the **Relocate Open Port Findings** setting, which simplifies how open ports are displayed across Tenable Vulnerability Management, unlocks new filters and tag rules, and speeds up your scan times.

Administrators can enable this feature in **Settings** > **General** > **Scanning**.

Relocate Open Port Findings does the following:

- Adds a new **Open Ports** tab on the **Asset Details** page for host assets.
- Adds a new **Open Ports** asset filter to the **Assets** workbench.
- Adds a new **Open Ports** tag rule to the **Tags** page.
- Adds the ability to export open port data from the **Assets** workbench.
- Disables the **High-Traffic Info Plugins** setting, which Tenable plans to retire.

For more information, see General Settings.

Workspace Page and Custom Role Enhancements

The **Workspace** page appears when you log in to Tenable. In addition, administrators can change which custom roles can access which Tenable One apps.

- To set a default app on the **Workspace** page, click on the app tile and select **Make Default Login**. To remove a default app on the Workspace page, click on the app tile and select **Remove Default Login Page**. The **Workspace** page now appears when you log in.

Trim Findings Export Data

Tenable Vulnerability Management now trims cells longer than 32,000 characters in Findings CSV exports so they will appear correctly in Microsoft Excel. To turn this feature off, select **Untruncated Data**.

For more information, see Export Findings.

Agent Profiles

Tenable has updated the Tenable Vulnerability Management user interface with the ability to create and manage agent profiles. You can use agent profiles to apply a specific version to your linked agents. This can be helpful for agent version testing; for example, you may want to schedule a testing period on a subset of your agents before upgrading all your agents to a new version. An agent profile allows you to apply a newer version to a subset of your agents for a limited time, and more broadly, allows you to upgrade and downgrade agents to different versions easily.

You can manage agent profiles in the **Profiles** tab under **Settings** > **Sensors** > **Nessus Agents** in the Tenable Vulnerability Management user interface.

> **Note:** You cannot set agent profiles to versions earlier than 10.4.1. Agent profiles do not affect agents on versions earlier than 10.4.1.

For more information, see Agent Profiles.

Enhanced Asset Hostname Detection

Tenable has made enhancements to asset hostname detection in Tenable Vulnerability Management. These enhancements may result in updated hostnames for some assets, which will appear in the Explore workbench following a new scan. In addition, CSV exports of asset scans will now properly display hostnames or FQDNs where applicable.

Show Finding and Asset Counts in Explore Workbenches

Tenable is pleased to announce that the Explore workbenches in Tenable Vulnerability Management now display your actual finding or asset counts when that number exceeds 1,000, instead of only stating that there are more than 1,000.

For more information on the Explore workbenches, see Explore.

Explore Unification for Tenable Vulnerability Management

- New look and feel for Explore workbenches - Tenable is pleased to announce redesigned Explore workbenches with a modern layout and user interface.
- Asset tiles - Choose an asset tile to filter what data is shown. Asset tiles display the count for each asset type, which is affected by the filters you are using.
- Data visualizations - On the **Assets** page, click **Show Visualizations** to view interactive visualizations that break down your assets across a number of metrics and update based on applied filters.
- Active filters - Your current filters display at the top of the page. To remove a filter, click the **X**. Click **Clear All** to remove all filters.
- Change the grid view - Select **Grid: Compact View** for the default row height or **Grid: Basic View** for an expanded row height.
- Select a date range - Choose a date range to filter your assets by **Last Seen**. Select **All Time** to clear the filter. This filter is not available in **Advanced** mode.
- Customize table columns - Select or deselect columns to show or hide them from your tables.
- Drag and drop columns to arrange them.
- View info-level severity findings - Turn on the **Include Info Severity** toggle to show information-level severity findings. This toggle is off by default.

For more information, see Explore.

Process High Traffic Info Plugins Setting

You can now enable or disable Tenable Vulnerability Management from processing Info-severity plugins with the **Process High Traffic Info Plugins** general setting. Disabling this setting can improve export performance and end-to-end processing times per scan.

For more information, see General Settings.

Triggered Scan History Update

For triggered scan histories, Tenable Vulnerability Management now shows a scan history entry for each 12-hour window of the past 7 days.

Create Custom Widgets for Explore Dashboards

The **Widget Library** page now includes a **New Custom Widget** button to create custom widgets for **Explore** dashboards. For more information, see Create Custom Widgets for Explore Dashboards.

Share Report Templates

You can now share report templates with other users within your organization. The shared report templates can be accessed from the **Shared Report Templates** tab. For more information, see the Share Report Templates in the *Tenable Vulnerability Management User Guide*.

Differential Plugin Updates for Linked Tenable Nessus Scanners

Reduced the size of the daily plugin updates that linked Tenable Nessus scanners receive from Tenable Vulnerability Management. This size reduction minimizes the bandwidth required for updates.

For more information, see Differential Plugin Updates in the *Tenable Vulnerability Management User Guide*.

Scan Progress Bar Improvements

For vulnerability management scans, you can now hover over the scan status to view more status information in a pop-up window, such as the number of targets scanned and the elapsed or final scan time.

The scan status bar has also been updated with a new status: **Publishing Results**. This status shows while Tenable Vulnerability Management processes and stores the scan results.

For more information, see Scan Status in the *Tenable Vulnerability Management User Guide*.