tenable™
network security

SecurityCenter 4.8.1 Release Notes

This document describes many of the changes that are included in SecurityCenter 4.8.1, as well as significant enhancements and notes for upgrading.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.8. Users upgrading from 4.7 and earlier must first perform an upgrade to SecurityCenter 4.8 before attempting to upgrade to version 4.8.1. Please refer to the SecurityCenter 4.8 Upgrade Guide for information about upgrading to SecurityCenter 4.8. Information about upgrading from SecurityCenter 4.8 to 4.8.1 is available in the SecurityCenter 4.8.1 Upgrade Guide.

SecurityCenter 4.8.1 only supports Nessus scanners 5.x or later. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes and LCE 4.2.x for complete feature compatibility.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

SecurityCenter-4.8.1-es5.i386.rpm	be84235d7c3836e0f931fd6395f55dae
SecurityCenter-4.8.1-es5.x86_64.rpm	aac1c12443978cb2c54ae3405bf70df1
SecurityCenter-4.8.1-es6.i386.rpm	de5786cde8fcba48e7bc9b7d95b88186
SecurityCenter-4.8.1-es6.x86_64.rpm	7d377cf6f3926f6ae7763e5db4e78eef

4.8 Features

Changes to Nessus Enterprise Cloud (formerly Perimeter Service) scan settings – A number of changes were made to streamline SecurityCenter and Nessus communication (changes are only applied to communication within the Nessus Enterprise Cloud). Some of these changes include:

- Larger scan chunks sent to scanner
- Out of service threshold increased
- Status polling interval increased

PCRE support for vuln text – Full PCRE support is now available when filtering on vulnerability text. This can be used in all areas of SecurityCenter where vulnerability queries are used including Vulnerability Analysis, Dashboard, Reporting, and Alerts.

Performance improvements for managing Reports and Dashboards – As the number of viewable dashboards and reports increased, the load time for the dashboard and report management pages became too long. Changes were made in the communication to significantly speed up those processes by only passing back the full query definitions for a report or dashboard when an edit was performed as opposed to on initial load.

Implement .k5login privilege escalation – To support new Nessus functionality, we have added the ability for a user to select ".k5login" as an option in the privilege escalation drop-down for SSH credentials.

Upgrade to PHP 5.4.28 – To address security issues within PHP, we have upgraded PHP to version 5.4.28.

Bug Fixes

- Resolved the issue where a rollover scan would continually copy itself over causing multiple scan jobs to execute over time.
- Addressed an issue with tag selection in the “Output Asset” filter.
- Fixed a bug that listed incorrect users within the User Responsibility Summary.
- Resolved the issue where the “Perform PCI DSS Analysis” checkbox is not enabled in the UI when adding a PCI DSS Scan policy template.
- Addressed the issue where a user was not able to log in to the HTML application using a CAC card.
- Fixed the bug that caused a PVS offline update to fail due to not being registered.
- Fixed the incorrect authentication settings for MSSQL Server
- Addressed the issue where certain credentials were being stored in the clear in the sc4-configuration.txt file.
- Resolved a user model bug in which a user is unable to delete an asset that is assigned as a “Responsible Asset” to a deleted user.
- Fixed a bug in the HTML application that would not allow a user to use the “combination of” functionality when filtering on an asset.
- Addressed the general error that was thrown stating “Please specify the list of assets” in the HTML application.
- Resolved the issue when trying to send a dashboard to a report and the vulnerability bar would not render.
- Fixed the bug where a filter that was applied on the “Assets” page persisted in filters on the “Analysis” page.
- Numerous other fixes.

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world’s largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com