Record ID: CCEVS-VR-VID10461-2013

CCEVS Approved Assurance Continuity Maintenance Report

Product:	McAfee Vulnerability Manager v7.5.4
EAL:	2 + ALC_FLR.2
Date of Activity:	9 October 2013
References:	CCIMB-2004-02-009 Assurance Continuity: CCRA Requirements, Version 1.0, February 2004 Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008 McAfee Inc. Vulnerability Manager v7.5.4 Common Criteria Assurance Maintenance Impact Analysis Report Version 0.2, Oct. 9, 2013.
Documentation Updated:	McAfee Inc. Vulnerability Manager v7.5.4 Security Target Version 0.1, September 18, 2013 Common Criteria Testing Results, August 29, 2013 McAfee Corporation Vulnerability Manager v7.5.4 Guidance Documentation Supplement Version 0.3, October 9, 2013 McAfee Installation Guide McAfee Vulnerability Manger 7.5, May 22, 2012 McAfee Product Guide McAfee Vulnerability Manger 7.5, May 24, 2012

I. Introduction

On October 9, 2013, McAfee Inc. submitted an Impact Analysis Report (IAR) to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation", 8 September 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

This is the second IAR approved based on the original evaluation. The summary of changes listed below represent the cumulative set of changes from the original evaluation. Two of the documents listed above as changed, the Installation Guide and the Product Guide, were not altered as a result of the current IAR but were altered by the previous IAR and hence are listed for completeness. Although the Installation Guide was not modified by the current IAR, the installation process is augmented with additional steps described in the Guidance Documentation Supplement.

II. Changes to the TOE

A list of the new features and enhancements to the TOE is provided in the Table below, along with the TOE version in which the feature or enhancement was first added, and a description of the change.

Feature Name	TOE Version	Description of Change
New Dashboard – Most Prevalent Vulnerabilities	7.5	Adds a new dashboard to the Web Interface, which displays the ten vulnerabilities with the highest number of occurrences.
New Dashboard – Most Prevalent Operating Systems	7.5	Adds a new dashboard to the Web Interface, which displays the ten operating systems with the highest number of occurrences, based on scanned assets.
New Dashboard – Vulnerability Count by Severity	7.5	Adds a new dashboard to the Web Interface, which displays the number of High, Medium, Low, and Information vulnerabilities.
New Dashboard – Vulnerability percentage	7.5	Provides a new monitor to the Web Interface that shows the percentage of

by Severity		High, Medium, Low, and Information vulnerabilities.
New Dashboard – Organization Vulnerability Count Trend	7.5	Adds a new dashboard to the Web Interface, which displays a trend graph of the High, Medium, Low, and Information vulnerabilities for the organization, over time.
IP7v6 Scanning	7.5	Allows scanning of target machines that have Internet Protocol version 6 (IPv6) addresses.
Scan Details Page	7.5	Adds a new page which shows the progress of different processing during a scan
Asset Tags and Organization	7.5	Gives Organization administrators the ability to create, assign, remove, and delete a tag (or name) to an asset.
Vulnerability Sets	7.5	Allows creation of a vulnerability set to target which vulnerabilities to scan for and generate reports for.
SUDO8 Scanning	7.5	Allows users to use SUDO instead of SU9 for running individual commands in privileged mode.
New Email Notifications for Scan and Scan Engine Events	7.5	Three new scan email notifications and one scan engine email notification can be used.
Ports in Reports	7.5	For general vulnerabilities and web FSL10 checks, the port number, service, and protocol are now included in the Vulnerability Details and Vulnerabilities by IP report sections.
Gather diagnostic info and logs task	7.5	Gathers log files of the TOE and other information to assist in troubleshooting by customer support.
Apply registry tweaks task Scan controller preferences tab	7.5	Applies registry tweaks from an XML11 file. Sets the maximum number of concurrent connections a scan controller can make to the database.
Scan controller preferences tab	7.5	Sets the maximum number of concurrent connections a scan controller can make to the database.

Scan engine preferences tab	7.5	Sets the maximum amount of time allowed for a post operation to get a response before the scan engine times it out
RealTime Scanning	7.5.1	Gives administrators the ability to run continuous scans of assets on the network. Only one RealTime scan can be assigned to a scan engine.
Operating System Identification	7.5.1	Allows administrators the ability to manually set the operating system identified on an asset. A priority can be applied to the asset based on the operating system.
McAfee Product Integration	7.5.1	Allows for McAfee Asset Manager the ability to send Vulnerability Manager asset information to improve the accuracy of scan results.
Vulnerability Information for Mobile Platforms	7.5.1	Allows mobile devices to be added as assets to the asset table and Asset Management page. When a scan is run, a list of known vulnerabilities related to the software versions running on the device can be presented to the administrator. Vulnerability Manager does not connect to the mobile device during a scan but identifies vulnerabilities based on the mobile device information.
ePolicy Orchestrator (ePO) Assets in the Assets Table	7.5.1	Allows ePO assets to be included with Vulnerability Manager assets. ePO assets can be added to a scan configuration from the Targets tab.
Microsoft Windows 8 and Microsoft Windows Server 2012 Assets	7.5.1	Allows administrators the ability to run scans that include assets running Microsoft Windows 8 or Microsoft Windows Server 2012.

Foundstone Attack Scripting Language (FASL)Editor	7.5.4	FASL is a programming language supported by Vulnerability Manager and is used to check systems for vulnerabilities. The FASL Editor provides administrators a new tool to create scans. CodeMirror has been integrated to format scripts for administrator convenience.
CyberScope Reports	7.5.4	. Provides administrators a new type of scanning report. CyberScope report increases reporting functionality including additional functionality to add up to three organizations to appear in the report and to filter data for a specific benchmark.
Filtering vulnerabilities in the Vulnerability Tree	7.5.4	Allows administrators to view only the vulnerabilities they have selected for the "Vulnerability Tree for a Vulnerability Set" or scan configuration
Faultline Identification (FID) included in Scan and Asset Reports	7.5.4	The FID number is now included in scan and assets reports for administrators to view.
Same Day Saved Reports Overwrite Protection	7.5.4	Prevents saved reports that are run on the same day from overwriting each other.
Telnet only option for Shell credentials.	7.5.4	Provides administrators the ability to select a Telnet only option to use for shell credentials. No cryptographic functionality has been changed otherwise.
View Active assets in the Dashboard	7.5.4	Provides administrators the ability to view only active assets in a new Active Asset View in the dashboard.

III. Analysis and Testing

CCEVS concluded that the change included in the IAR did not have greater security impact than was reported, and that it could be classified as minor. No new security features are added and no Security Functional Requirements needed to be changed on account of the changes included in the IAR. No major changes were required in the ST. Regression testing was conducted to verify that no security-relevant changes in TOE operation were observed. The result of the testing were reported in the updated Testing Report.

IV. Conclusion

The changes to the TOE is confined to user interfaces to improve the usability of the product. No existing security functionality was removed and no new security functionality was added.

The changes are classified as minor, and certificate maintenance is the correct path for assurance continuity, therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.