Record ID: VID10486-0004-ACMR

CCEVS Approved Assurance Continuity Maintenance Report

Product:	McAfee Endpoint Encryption PC v7.0 with McAfee ePolicy Orchestrator 4.6
EAL:	2 augmented with ALC_FLR.3
Date of Activity:	25 March 2013
References:	Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008 McAfee Endpoint Encryption PC v7.0 with McAfee ePolicy Orchestrator 4.6 Impact Analysis Report, Version 1.0, 18 February 2013
Documentation Updated:	McAfee Endpoint Encryption PC v7.0 with McAfee ePolicy Orchestrator 4.6 Common Criteria EAL2+ Security Target, 9 February 2013, version 017 McAfee Endpoint Encryption 7.0 for PC with McAfee ePolicy Orchestrator 4.6 Common Criteria EAL2+ Configuration List, 18 February 2013 McAfee Endpoint Encryption 7.0 for PC with McAfee ePolicy Orchestrator 4.6 Common Criteria EAL2+ Functional Specification, 09 February 2013, version 003 Product Guide McAfee Endpoint Encryption 7.0 For use with ePolicy Orchestrator 4.6 Software, 2012 McAfee Endpoint Encryption 7.0 for PC with McAfee ePolicy Orchestrator 4.6 Common Criteria EAL2+ Administrative Guidance and Preparative Procedures Supplement, 09 February 2013, version 004 McAfee Endpoint Encryption for PC with McAfee ePolicy Orchestrator Common Criteria EAL2+ Functional Test Specification – Win7 x86, 10 February 2013, version 002 McAfee Endpoint Encryption for PC with McAfee ePolicy Orchestrator Common Criteria EAL2+ Functional Test Specification – Win8 x64, 13 February 2013, version 002

I. Introduction

On 18 February 2013, McAfee submitted an Impact Analysis Report (IAR) for Endpoint Encryption PC v7.0 with McAfee ePolicy Orchestrator 4.6 to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 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.

II. Changes to the TOE

The primary reason for the Assurance Continuity activity for MEE PC 7.0 is the support of Windows 8 Endpoint PC clients.

The most important change in the MEE PC 7.0/ePO 4.61 TOE (from MEE PC 6.2/ePO 4.62) is:

Windows 8 support – There are two variants of the product configuration supported on Windows 8

- **Legacy BIOS Preboot environment** – This configuration is the same as that used for Windows 7 as certified for MEE 6.2 (as detailed in [MEE62_ST]). This configuration uses the FIPS validated crypto libraries as used in the MEE PC 6.2 evaluation specified in [MEE62_ST]. Therefore, this change is considered to be minor.
- **UEFI Support in Preboot environment** – This configuration uses a new boot process, PBA environment and crypto library and hence is not supported in the evaluated configuration and this change is considered to be minor.

The following enhancements have been made to the MEE PC 7.0 firmware between MEE PC 6.2 and MEE PC 7.0:

- **MEE Out of Band Management** – There are three new features providing Out Of band management (Remediation, Unlock PBA and User Management) that rely on the AMT chip. Use of these features is not supported in the evaluated configuration. Therefore, these changes are considered to be minor.
- **Near native performance** – This relates to the improvements to an AES-NI algorithm, applied to the new crypto libraries. These new crypto libraries are not used in the evaluated configuration, which requires the product to the installed in FIPS mode (which installs the FIPS validated crypto libraries integrated in MEE 6.2, as specified in [MEE62_ST]). Therefore, this change is considered to be minor.
- **Hardware entropy source** – This relates to the crypto libraries' use of Intel RdRand instruction as a source of entropy. These new crypto libraries are not used in the evaluated configuration, which requires the product to the installed in FIPS mode (which installs the FIPS validated crypto libraries integrated in MEE 6.2, as specified in [MEE62_ST]). Therefore, this change is considered to be minor.
- **Offline Activation** – This functionality is used when a 3rd party is responsible for provisioning a machine with an encrypted hard disk. As the 3rd party does not have access to ePO, this provides a method of protecting the created DEK.

However, use of this offline activation feature is not supported in the evaluated configuration. Therefore, this change is considered to be minor.

- **Support of biometric tokens for authentication** – The support of tokens for authentication was provided in MEE PC 6.2. This change just extends the list of supported tokens. Therefore, this change is considered to be minor.
- **EEGo** – This new tools spiders the network, querying connected workstations/laptops to report any incompatibility or potential issues with installing MEE PC on the workstation/laptop. This tool is used prior to installation of the TOE on the workstation/laptop and is not relevant to any of the security functional requirements specified in [MEE62_ST]. Therefore, this change is considered to be minor.
- **Pre-boot Smart Check** – This policy option runs at activation time iterating through possible configurations of MEE (in accordance with specified policies) prior to encrypting the workstation disk to ensure the disk is not encrypted when there is a compatibility issue with the configuration of the workstation that may render the data inaccessible. Once a good configuration is found, it is used thenceforth. If no good configuration is found, MEE is deactivated. Use of this policy option is not supported in the evaluated configuration, and therefore, this change is considered to be minor.
- **WACOM support** – Support of serial WACOM driver for use of a tablet pen during preboot was provided in MEE 6.2. This extends that support for use of USB pens also. This change does not relate to any of the security functionality as specified in [MEE62_ST]. Therefore, this change is considered to be minor.
- **GPT Drive support** – In MEE 6.2 the address space for disk access was limited to 32 bits, meaning disks larger than 2.8TB were not supported. In MEE 7.0 the 32 bit integer has been extended to a 64 bit integer to support large GPT drives. The mechanism for disk access is unchanged, only the size of integer used for LBA addressing has increased (32 to 64 bits). Therefore, this change is considered to be minor.
- **Export recovery information based on Disk Keycheck** – The ability to export a DEK was available via an API in MEE 6.2. This change has merely added the capability to the ePO UI. The same data is available for export through this MEE 7.0 ePO extension interface, and the key is exported using the same file format. Therefore, this change is considered to be minor.
- **Require Endpoint Encryption Logon** – This functionality has been removed (this does not relate to MEE pre-boot authentication; but rather it relates to MEE's Credential Provider and GINA which provided Windows authentication). This change does not affect any of the security functionality specified in [MEE62_ST] and therefore is considered to be minor.
- **Enhanced Administrator Recovery** – This functionality relates to the information that can be gained during pre-boot. If the user forgets their password

and needs to go through administrator controlled recovery using the MEE Out-of-band Management password recovery (item , above), the machine ID can be gained from the pre-boot "About" screen in order to help the administrator to identify the machine to manage. This data is not considered to be sensitive and therefore, this change is considered to be minor.

- **Encryption Status Monitor** – During encryption of the disk (following installation) a status window can be displayed. This status window has been enhanced to display the percentage of disk encryption completed. This data is not considered to be sensitive and the enhancement is security irrelevant to the disk encryption function that is in progress at the time (it is unable to affect the behavior of the function performing the disk encryption). Therefore, this change is considered to be minor.

- **WinPE4** – WinPE4 is required for UEFI. As support of UEFI platforms is not supported in the evaluated configuration (see item #1 above), this functionality is not available in the evaluated configuration and is therefore considered to be minor.

- **Crypto for (UEFI platforms for) Windows 8** – The crypto libraries used for UEFI platforms have been modified (these libraries have not yet been through FIPS validation). However, as support of UEFI platforms is not supported in the evaluated configuration (see item #1 above), these libraries are not available in the evaluated configuration. Therefore, this change is considered to be minor.

- **Re-organisation of Guides** – The scope of the Product Guide and the Scripting Guide have been extended to cover MEE PC 7.0 and any platform specific documentation needed for MEE Mac 7.0.. Additional information relating to installation (including offline installation), use of biometric tokens and recovery have been provided in the Product Guide. The reorganization of the product guides and the additional information required to support the minor changes in MEE PC 7.0 as described above are considered to be minor.

The following enhancements have been made to ePO 4.6 firmware between ePO 4.6 patch 2 and ePO Patch 4:

- **ePO Improved Dashboards** – The colors and fonts used in the ePO Dashboards have been updated to increase legibility. The MyAverts Threat Advisory dashboard has been replaced with the McAfee Labs dashboard to provide accurate information from McAfee Labs and multiline charts can be sorted by value. None of these changes relate to the security functionality specified in [MEE62_ST]. Therefore, these changes are considered to be minor.

- **ePO corrections** – Releases 4.6.3 and 4.6.4 of ePO incorporate a number of corrections to documented ePO functionality. As these changes are to correct the implementation and behavior of ePO to match the documented design, these changes are considered to be minor.

III. Analysis and Testing

The test cases used for the original evaluation were successfully re-run with slight modifications to cover new biometric identification credentials and the new operating system. The vendor analysis shown in Section II supports the conclusion that only minor security affects to the evaluated configuration have resulted from the product updates.

IV. Conclusion

This maintenance activity covers the assessment of the evaluation impact of the changes applied to McAfee Endpoint Encryption PC v7.0 with McAfee ePolicy Orchestrator 4.6.

The listed changes for McAfee Endpoint Encryption PC v7.0 with McAfee ePolicy Orchestrator 4.6 show that small changes to the I&A functionality and the addition of a new supported operating system. Therefore the conclusion is that the changes are acceptable under the assurance maintenance program.

The following additional guidance is provided to emphasize which features should not be used in the evaluated configuration as the result of these changes. See the updated ST and guidance document for further details.

- UEFI Support in Pre-boot environment should not be used in the evaluated configuration.
    - WinPE4 is not available without UEFI
- MEE Out of Band Management should not be used in the evaluated configuration.
- The product should only be used in the FIPS mode which means the new features of improved or extended crypto use cannot be used in the evaluated configuration:
    - Near native performance
    - Hardware entropy source
    - Crypto for (UEFI platforms for) Windows 8
- Offline Activation should not be used in the evaluated configuration.
- Pre-boot Smart Check should not be used in the evaluated configuration.

In addition, it is important for the user of this product to review the original Validation Report Sections 4 and 10 and the new ST to understand the limitations on the evaluated configuration.