Maintenance Report

McAfee Change Control and Application Control 6.2.0 with ePolicy Orchestrator 5.1.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-123 MR
Version: 1.0
Date: May 14, 2015
Pagination: 1 to 2

1 Introduction

McAfee, Inc. has submitted, via Primasec, the Impact Analysis Report (IAR) for McAfee Change Control and Application Control 6.2.0 with ePolicy Orchestrator 5.1.1 (hereafter referred to as McAfee Change Control and Application Control), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in McAfee Change Control and Application Control, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes in the Maintained Target of Evaluation

The following characterizes the changes implemented in McAfee Change Control and Application Control. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained. The changes in McAfee Change Control and Application Control comprise the following:

- Enhancements to the administrative interface including the health monitoring dashboard, permissions enforcement, inventory view customization and policy creation;
- Traffic flow control with throttling to improve responsiveness of the ePolicy Orchestrator interface;
- McAfee Agent performance enhancements such as peer to peer communication, remote provisioning and persistent connection for agent to server communication;
- Application of Hotfix 1038703 for the ePolicy Orchestrator which addresses reported security vulnerabilities in Java and was produced in response to CVE 014-3566, CVE 2014-6593 and CVE 2015-0410;
- The version of Java in use for the ePolicy Orchestrator was updated to Java JRE 1.7_76;
- The cryptographic module used in the McAfee Agent has been updated to a more recent version. The new module was validated against FIPS 140-2 (certificate #2097); and
- Bug fixes resulting from defects detected and resolved through the QA/test process.

There were no changes to the underlying IT environment.

3 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions and typographical errors.

4 Conclusions

Through functional and regression testing of McAfee Change Control and Application Control , assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

5 References

- Assurance Continuity: CCRA Requirements, v2.1, June 2012;
- CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011;
- Certification Report for McAfee Change Control and Application Control 6.1.3 with ePolicy Orchestrator 5.1.1, v1.0, 24 November 2014; and
- McAfee Change Control and Application Control v6.2.0 with ePolicy Orchestrator v5.1.1 Security Target, Version 2.1, 29 April 2015.