



CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR McAfee IntruShield Intrusion Prevention System

Maintenance Update of McAfee IntruShield

Maintenance Report Number: CCEVS-VR-VID10169-2009a

Date of Activity: 2 Jun 2009

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Impact Analysis Report for Common Criteria Assurance Maintenance Update of McAfee IntruShield

Documentation Updated: (List all documentation updated)

- Security Target for IntruShield Product Family
- Functional Specification
- High Level Design
- Configuration Management Plan
- Test Plan
- Vulnerability Analysis
- Administrative Guidance

Assurance Continuity Maintenance Report:

The vendor for the IntruShield Intrusion Prevention System, McAfee Incorporated, submitted an Impact Analysis Report (IAR) to CCEVS for approval on May 19, 2009. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. 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.

Changes to TOE:

The changes to the TOE consisted of 17 minor fixes. Each fix was applied to make the TOE or supporting hardware/software function as originally intended, no additional security functionality was added, and no existing security functionality was removed.

Each of the fixes fall into the following categorizations:

- **Minor Changes with Little or No Security Relevance:** These changes may be related to the TSC in some way, though may or may not relate directly to an SFR defined within the ST. These include bug fixes for vulnerabilities discovered after evaluation.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

- **Minor Changes with Some Security Relevance:** These changes relate to the TSC in some way though the affect of the change is only to ensure the TOE functions as expected, and does not add or detract from the stated requirements in the ST.

The IAR provided by McAfee indicates that the assurance evidence has been updated to reflect the changes, and appropriate testing of the changed TOE has occurred.

In addition to the software changes to the TOE, this maintenance release adds two new sensor hardware models (M-6050 and M-8000) sensors to the evaluated configuration. These additional platforms execute the same software image as the maintained TOE. In addition, the vendor provided updated test documentation covering the new hardware and providing additional assurance that the maintained TOE continues to satisfy the original requirements. In addition, the existing I-3000 and I-4010 sensor models now provide support for gigabit Ethernet interfaces. These changes were judged to be below the level of the original TOE evidence and therefore acceptable for maintenance.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.