CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
HIP V.7.0 and ePolicy Orchestrator V.3.6.1 Patch 1
Maintenance Report Number: CCEVS-VR-07-0030a

Date of Activity: 07/21/2008

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

Impact Analysis Report,” F3-0308-002 Impact Assessment Report for: HIP (Version 7.0) and ePolicy Orchestrator (Version 3.6.1 patch 1), Dated March 28, 2008

Documentation Updated: McAfee Host Intrusion Prevention (HIP) v6.0 for use with ePolicy Orchestrator (EPO) v3.6 Installation/Configuration Guide

McAfee® Host Intrusion Prevention version 6.0 Product Guide

McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 (Patch 1) Security Target, May 2007

Host Intrusion Prevention 6.0.2 Supplementary Documentation

McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 (Patch 1) developer evidence

Assurance Continuity Maintenance Report:

The vendor for the McAfee HIP 6.0.2 and ePolicy Orchestrator 3.6.1 (Patch 1) submitted an Impact Analysis Report (IAR) to CCEVS for approval on 10 April 2008. 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 increase the performance of policy enforcement and communication between the agents and the server, update the Operating Systems supported, and allow administrators to test policies before pushing them out to agents. The one item that would have an effect on the security functionality is disabled by default and there are warnings in the administrator guidance to keep the function disabled.

While there were other significant changes made to the product, they apply to the firewall portion of the product. The firewall portion of the product is outside the TOE boundary in the original Validated Product.

Conclusion:

The changes to the TOE environment were analyzed and found to have no effect on the security of the evaluated TOE. The non-security relevance of the changes leads to the conclusion that the updates can be classified as a **minor change** and that certificate maintenance is the correct path for continuity of assurance.