CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

HP ArcSight Enterprise Security Management 6.0c Patch 1

Maintenance Report Number: CCEVS-VR-VID10423-2014

Date of Activity: 9 June 2014

References: Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 2, September 8, 2008

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 1, February 2004

HP ArcSight Enterprise Security Management (ESM) Impact Analysis Report, Revision 1.1, 05/15/2014

Documentation Updated: ArcSight ESM 6.0c Patch 1 Security Target Version 3.0, May 30, 2014

Common Criteria Evaluated Configuration Guide: ArcSight ESM 6.0c Patch 1; June 6, 2014

ArcSight Console User's Guide: ArcSight ESM 6.0c

ArcSight ESM Administrator's Guide: ArcSight ESM 6.0c

Assurance Continuity Maintenance Report:

Leidos acting for HP Corporation, the vendor of "HP ArcSight Enterprise Security Management", submitted an Impact Analysis Report (IAR) to CCEVS for approval in May 2014. 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.

Changes to TOE:

TOE Changes:

- Total Changes included in IAR – 384;
- Changes with major security relevance – 0;
- Changes relevant to the TOE – 229; and
- Changes out of scope to the TOE - 155

Types of Changes:

- Software changes – the most significant software change was the removal of reliance on an external relational database management system (Oracle) and substitution of an internal data management system (CORR-Engine). This change eliminated interfaces to the Oracle dbms and altered certain administrative functions that had Oracle-specific syntax. The existing data schema and overall administrative operations regarding that data schema were not altered. No new functions were introduced and the observable behavior of the TOE did not change. Evaluation test cases that included Oracle-specific commands were changed to reflect the appropriate CORR-Engine commands.

  Other software changes included regular updates to the JAVA Runtime Environment (JRE), released by the JAVA vendor, to address published JRE vulnerabilities. Other changes addressed reported performance issues as well as updates to user commands to optimize and simplify operations and improved ease of use. None of these changes introduced any new features or otherwise changed any TSFIs.

- Documentation changes – the removal of the Oracle RDBMS and the addition of the CORR-Engine required changes to be made in the ST, appropriate installation guides, and associated configuration documents. Other documentation changes corrected or added clarifying information but did not involve any code changes. Documentation changes also were made to reflect the change of corporate ownership from ArcSight to HP and to accommodate the replacement of ArcSight internet services with those provided by HP (e.g., replacement of ArcSight web-addresses with those of HP).

- Changes out of scope to the TOE included such things as: adding enhancements for services such as support of IPv6 that were not include in the original evaluation; support of pre-configured lists, filters, and channels, etc.; changes to MS Windows commands because support of Windows was removed from the TOE; support of non-English language fonts that were not included in the original evaluation, and fixes and work-arounds, such as edits to “properties files”, that are not allowed in the evaluated configuration.

The most significant software change made to the TOE was done in response to performance issues regarding the support of the external Oracle RDBMS. Replacement with the CORR-Engine simplified the design and operation of the TOE as well as provided significant performance improvements. It also simplified installation and establishment of the evaluated configuration.

The change was considered to have only minor impact because it required no alteration to TOE interfaces, only minimal modification to the database, and had no visible impact during testing. The mechanisms used to access the database and submit commands only changed with the replacement of Oracle specific commands with ones for the CORR-Engine. Administrative documents were appropriately updated including warnings in the evaluation configuration guide to create only TOE Administrator accounts on the host platform system.

Complete regression testing was conducted and certain tests that included Oracle-specific commands and syntax required modifications. This necessitated a full Test Case Analysis and that was performed.

CCEVS concluded that the changes included in the IAR did not have greater security impact than was reported, and that none of them could be classified as major. No new security features were added, no Security Functional Requirements needed to be changed on account of the changes included in the IAR, and no user-perceptible changes were made.

Conclusion: The changes to the TOE were to software and documentation and some were out of scope. The vendor claims that testing of the specific changes was done and regression testing was also conducted. Those test logs and supporting evidence were not provided in the IAR package.

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.