CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Aruba Mobility Controller and Access Point Series, ArubaOS 3.4.4.0-FIPS

Maintenance Report Number: CCEVS-VR-VID10348-2012

Date of Activity: 23 August 2012

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

Impact Analysis Report, Aruba Mobility Controller and Access Point Series, Version 1, rev. 2

Documentation Updated: Aruba Mobility Controller and Access Point Security Target, Version 1.1, June 11, 2012

ArubaOS 3.4.4.0 Release Notes: http://support.arubanetworks.com/DOCUMENTATION/tabid/DMXModule/512/EntryId/7518/Default.aspx

Aruba Common Criteria EAL 4 | Addendum

Assurance Continuity Maintenance Report:

SAIC submitted an Impact Analysis Report to CCEVS for approval on June 11, 2012 on behalf of the vendor; Aruba Networks, Inc. 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" Version 2, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence that was updated as a result of those changes, and the security impact of those changes.

Changes to TOE:

Aruba has revised the firmware OS in their hardware appliances from ArubaOS 3.4.2.3 to ArubaOS 3.4.4.0. ArubaOS 3.4.4.0-FIPS represents a number of standard maintenance fixes to address bug fixes, device driver and protocol handling issues along with minor appearance changes and other optimizations. The release has been FIPS validated and all FIPS certificates have been updated with the new validation date of 07/19/2011 for ArubaOS 3.4.4.0-FIPS.

Four of the changes were security related: the addition of Kerberos authentication support, NAT-T changes to support MAC clients, NTP authentication, and management password policy enhancements. The vendor chose to explicitly exclude those from evaluation and the Security Target has been updated to reflect those exclusions.

Conclusion: The changes to the TOE are confined to firmware. It should be noted that the following security related changes were specifically excluded and were not evaluated:

- Kerberos authentication support
- NAT-T changes to support MAC clients
- NTP authentication
- Management password policy enhancements

Therefore the use of those functional components to manipulate the TOE functions and data when the TOE is operational removes the TOE from the evaluated configuration.

The changes are classified as minor, and certificate maintenance is the correct path for assurance continuity, (noting the specific exclusions put forth above) therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.