ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Aruba Remote Access Points

Maintenance Update of Aruba Remote Access Points

Maintenance Report Number: CCEVS-VR-VID10766-2017a

Date of Activity: September 26, 2017

References:

Aruba Remote Access Point Version 6.5.1-FIPS Security Target, Version 1.1. September 26, 2017.

Aruba Remote Access Point Impact Analysis Report, Revision 0.1. September 26, 2017

Aruba Remote Access Point, ArubaOS 6.5.1-FIPS Common Criteria Configuration Guide, Version 1.4. June, 2017.

ArubaOS 6.5.1.x User Guide

ArubaOS 6.5.1.x Command-Line Interface

Documentation reported as being updated:

Table 1 Updated Documentation

Original Document Title	Updated Document Title
Aruba Remote Access Point Version 6.5.0-FIPS Security Target, Version 1.0, 02/09/2017	Aruba Aruba Remote Access Point Version 6.5.1-FIPS Security Target, Version 1.1, 09/26/2017
ArubaOS 6.5.0.x User Guide, Revision 5, September 2016	ArubaOS 6.5.1.x User Guide, Revision 0.3, November 2016
Aruba VPN Client Protection Profile, Common Criteria Configuration Guide Version 1.3, November 2016	Aruba VPN Client Protection Profile, Common Criteria Configuration Guide Version 1.4, June 2017
ArubaOS 6.5.0.x Command-Line Interface Reference Guide, Revision 2, September 2016	ArubaOS 6.5.1.x Command-Line Interface Reference Guide, Revision 3, January 2017

Assurance Continuity Maintenance Report:

Aruba submitted an Impact Analysis report (IAR) to the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for approval. 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 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The IAR identifies the changes to the TOE, which include all changes made to the Aruba Remote Access Point Version 6.5.0-FIPS product evaluation (CCEVS-VR-VID10766-2017) to update it to the current version (Aruba Remote Access Point Version 6.5.1-FIPS). In addition to general bug fixes, the updates included the addition of new features, software optimizations, and appearance changes. Some of the software updates were security-relevant, but outside the scope of the evaluation. In addition, support for another appliance model (AP-205H Access Point) was added to the TOE. The product changes resulted in documentation updates, including changes to the Security Target (ST), and changes to guidance documentation comprised of the User Guide (UG), Common Criteria Configuration Guide (AGD), and Command Line Reference Guide (CLI AGD).

Changes to the Security Target included updating the ST identifier and the TOE identifier; adding the appliance model (AP-205H Access Point); updating the list of CAVP and CMVP certificates that are applicable to the TOE (CMVP Cert #3021 and #3023); updated the ST to reflect that SHA256 is now the algorithm used to perform integrity checks; and updating the list of guidance documents. Changes to the guidance documentation includes updates to reflect new TOE features and modifications of existing features, as well as information about bug fixes.

Changes to TOE:

Aruba has provided several updates to the ArubaOS, the operating system for all of Aruba's controller-managed wireless LAN devices, including the TOE. TOE updates largely consisted of a variety of bug fixes, modifications to the user interface, and performance optimizations none of which were security-relevant. However, some modifications to ArubaOS were security-relevant, while others are security-relevant, but out of scope for this evaluation. The following are a summary of the security-relevant changes to ArubOS and a brief discussion of their impact on the assurance maintenance of the TOE.

- **Support for SHA2 Signature for Image Verification**

The controller images now support SHA256 signatures for image verification. While copying new images to the controllers, both SHA1 and SHA256 signatures are validated.

Minor Change: *The original evaluated TOE implemented both SHA1 and SHA256, but chose to call on the SHA1 algorithm to perform the code integrity verification check. RSA with SHA256 was already supported/tested in the ArubaOS Crypto Module for Trusted Updates and in conjunction with HMAC for authentication of IPsec connections. The updated TOE has been changed to call on the SHA256 algorithm (already implemented in the previous version, and validated by NIST testing) to perform the code integrity check. Since this change only involves invocation of the underlying cryptographic mechanism, it is considered a minor change. This feature results in no changes to*

TSF platforms, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment.

- **Revocation of ArubaOS Default Certificate Issued by GeoTrust**

The controller-issued server certificate replaces the ArubaOS default certificate issued by GeoTrust Public CA for WebUI authentication, Captive Portal, 802.1X termination, and Single Sign-On (SSO) because the default certificate is now revoked.

The revoked default certificate is applicable to Aruba Mobility Controllers, Instant Access Points (IAP) and Mobility Access Switches (MAS).

For more information on the GeoTrust Public CA certificate revocation, refer to the advisory: http://community.arubanetworks.com/t5/Controller-Based-WLANs/ArubaOS-Default-Certificate-Revocation-FAQ-Controllers/ta-p/275809.

***Minor Change** –The revoked default certificate is not applicable to the TOE.*

- **Support for OCSP and USB Custom Certificate on AP-205H**

Starting from ArubaOS 6.5.1.0, support for Online Certificate Status Protocol (OCSP) and USB custom certificate is introduced on AP-205H remote access points. With this feature:

- AP-205H remote access points support checking the revocation status of the controller certificate by reading the AIA field of the server certificate with its corresponding OCSP responder.
- AP-205H remote access points can store CSR and private key files and read the custom certificate stored in .p12 certificate format for establishing IKE/IPsec tunnel with a controller.

***Minor Change** –The previous evaluation supported the OCSP feature for RAPs using ArubaOS 6.5.0. This feature was previously tested on the other models for 6.5.0. The 'added support' for the feature is only on AP-205H model that is being added through this assurance maintenance. It is considered a minor change because the functionality was already tested on the previous models. USB storage for custom certificates was supported in 6.5.0 but not included in the scope of the evaluation and therefore this feature addition for the AP-205H is considered a minor change.*

- **Null Encryption**

Starting from ArubaOS 6.5.1.0, XLP based controllers are supported with null encryption for IKEv1 as an encryption algorithm. This helps in reducing the load on the local router for internet destined traffic.

***Minor Change** –Controllers are not in the TOE. This support for reducing the load does not affect the security functionality of the TOE or modify any of the SFRs. The addition of this feature results in no changes to TSF platforms, SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment.*

- **ANY-ANY Crypto Map**

Starting from ArubaOS 6.5.1.0, any-any selectors are negotiated in IKEv1 to enable the option of having numerous tunnels. After pre-connect flag is enabled for IPsec map, IKE triggers the tunnel to the peer ip and proposes any-any traffic selector.

***Minor Change** –This feature is on Controllers only and does not affect the security functionality of the TOE or modify any of the SFRs. The addition of this feature results in no changes to TSF*

platforms, SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment.

PAPI Enhanced Security

Starting from ArubaOS 6.5.1.0, a minor security enhancement is made to Process Application Programming Interface (PAPI) messages. With this enhancement, PAPI endpoints authenticate the sender by performing a sanity check of the incoming messages using MD5 (hash).

All PAPI endpoints—access points, Mobility Access Switches, controllers, Analytics and Location Engine (ALE), AirWave, and HPE switches—must use the same secret key.

The PAPI Enhanced Security configuration provides protection to Aruba devices, AirWave, and ALE against malicious users sending fake messages that results in security challenges.

The PAPI Enhanced Security feature can be configured from either the WebUI or the CLI.

Minor Change – *Process Application Programming Interface (PAPI) is not in the TOE. This enhancement does not affect the security functionality of the TOE or modify any of the SFRs. The addition of this feature results in no changes to TSF platforms, SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment.*

- **Authentication Survivability**

The Cache Lifetime parameter value in Authentication Survivability is increased from 72 hrs to 168 hrs.

Minor Change – *Authentication Survivability is not within the scope of the TOE. The change in parameter values does not affect the security functionality of the TOE or modify any of the SFRs. This performance enhancement results in no changes to TSF platforms, SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment.*

Vulnerability Assessment:

The vendor conducted a vulnerability assessment to identify vulnerabilities that may affect the TOE. The search was scoped to the period after October 19, 2016.
The vulnerability assessment included a search of several vulnerability databases, including:

- https://web.nvd.nist.gov/
- http://www.securityfocus.com/vulnerabilities
- http://www.kb.cert.org/vuls

No vulnerabilities were discovered that affected the TOE that had not been mitigated or corrected in the TOE.

Regression Testing:

Aruba performed regression testing to commercial standards as part of approving implemented changes. Aruba incorporates automated testing into the build process and worldwide builds are performed nightly. The testing is cumulative and so therefore is exactly like the original tests (except for items removed), with tests for new features added. Aruba also includes tests developed specifically for demonstrating CC functionality in the automated suite. Additionally, regression testing is performed as part of the testing for FIPS 3SUB certification.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found them all to be minor. The addition of a new appliance model (AP-205H Access Point) and the software changes identified do not affect the security claims made in the Security Target. The new cryptographic module references have been assessed to be valid and applicable to the TOE. All evaluation evidence, including relevant guidance documentation, has been updated to reflect modifications made to the ArubaOS.

CCEVS has reviewed the description and analysis of the vulnerability assessment and has concluded that the vulnerabilities identified have been addressed and/or mitigated with the updates to the TOE. CCEVS has also reviewed the description of regression testing of the updated software and has concluded that the testing is adequate. Therefore, CCEVS agrees with Aruba that assurance is maintained for the product.