ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Aruba Virtual Intranet Access (VIA) Client Version 4.4

Aruba Virtual Intranet Access (VIA) Client Version 4.4

Maintenance Report Number: CCEVS-VR-VID11303-2023

Date of Activity: 24 January 2023

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Impact Analysis Report for Aruba, A Hewlett Packard Enterprise Company, Virtual Intranet Access (VIA) client, Revision .5, January 20, 2023
- Aruba Virtual Intranet Access (VIA) Client Version 4.4 Security Target, Version 1.3, 2023-01-18
- Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance, Version 1.3, September 2022
- PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.0, 2021-08-13, which includes the following:
    - Protection Profile for Application Software, version 1.3, 2019-03-01
    - PP-Module for Virtual Private Network (VPN) Clients, version 2.3, 2021-08-10

Assurance Continuity Maintenance Report:

Aruba, A Hewlett Packard Enterprise Company, submitted an Impact Analysis Report (IAR) for the Aruba Virtual Intranet Access (VIA) Client (was Version 4.3, updated to Version 4.4) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on January 20, 2023. 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 evaluation evidence submitted for consideration consists of the Security Target (ST), the Administrator's Guide, and the Impact Analysis Report (IAR). The ST and Admin Guide were updated to the new version of the TOE.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Aruba Virtual Intranet Access (VIA) Client Version 4.3 Security Target, Version 1.0, 08/23/2022	Updated to identify the new TOE version number.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance, version 1.2, March 2022	The administrator guide was revised to refer to the current product version and release notes for the current version.
Lifecycle: None	No changes required.
Testing: None	No changes required. Aruba has performed regression testing on 4.4 and all platforms in the ST have been subject to testing. This regression testing is conducted by the dedicated Quality Assurance team, in accordance with the Common Criteria requirements, to ensure no previous functionality has been impacted.
Vulnerability Assessment: None	The public search was updated from 8 August 2022 to 20 January 2023. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The TOE has been updated from VIA Client Version 4.3 to Version 4.4. Below is a summary of the changes.

<u>Major Changes</u>

None.

<u>Minor Changes</u>

Eighteen changes were identified in the IAR along with a description and given rationale. Fourteen of those changes impacted the VIA client on the evaluated platforms. The description and rationale for each were inspected and the overall Minor Change characterization was considered appropriate. None of the changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary. The following table includes a summary of the changes presented in the IAR that impact VIA and/or one or more of the evaluated platforms. The changes have been categorized according to Bug Fixes and Functional Updates.

Changes identified in the IAR that do not impact the evaluated platforms were also reviewed and have been included at the end of the Table.

Change Description	Affected Platforms	Assessment
Bug Fixes		
A VIA connection failed with the error **heart beat failed** was resolved in VIA 4.4	Windows	This is a bug fix and does not affect any SFRs.
Fixed VIA clients being unable to connect to the VPN while using existing user certificate (EAP-TLS). The issue was specific to user deployment.	Windows	This is a bug fix for an edge case in a specific customer environment.
Fixed an issue prior to VIA 4.3 related to the IKE handshake, which prevented the phase-2 proposal from being sent. The issue is resolved in 4.4, so upgrades to 4.4 will not be impacted by the issue	Windows	This bug is outside the scope of the relevant protection profiles and unrelated to any SFRs.
Improved how VIA manages the GUI if the registry is corrupted, allowing users to resume normal VIA functionality	Windows	This bug fix is unrelated to any SFR.
Changes to VIA 4.4 allow VIA to install the fonts file if missing from specific Windows client machines, resolving UI issues.	Windows	This bug fix is purely a UI/UX issue and is out of scope of the ST or the protection profile.
Functional Updates		
Display of warning message for the Windows client during profile download was fixed.	Windows	Profile download is outside the scope of the ST. This change therefore does not affect the compliance status of the TOE.
VIA 4.4 server certificate validation is done before profile download and if the certificate has changed, the user is shown a warning message about the change.	Windows	HTTPS connection is used for the configuration profile download which is handled by the platform operating system. Therefore, it is outside the scope of the ST. Overall product security is enhanced by this change, without impact to SFRs in the ST.
Improvements to VIA 4.4 clients to ensure they hold the profile download session for 2 minutes (or until the user provides a response, if less than two minutes)	iOS macOS Linux	Profile download is outside the scope of the Security Target or TSF.

Fixed issue in VIA 4.3 impacting entry of MFA-based authentication credentials. The issue was resolved for Android and iOS in VIA 4.4. (This was resolved for Windows Clients in 4.3.).	Android iOS Windows	Multi-factor authentication is out of scope of the relevant protection profiles. In addition, iOS is not claimed as an evaluated platform.
Fixed issue that allowed VIA clients to disconnect prior to the maximum session timeout period.	Windows	This bug fix corrects an issue that prevents a session from lasting to the maximum period. Being less than a maximum is not relevant to any security functional requirement.
The DN profile feature in VIA enables VIA had a strict check against all four identifiers; Common Name, Organization, Organizational Unit (OU), and Country. Starting with VIA 4.4, the Organizational Unit (OU) is optional. If the OU is absent, VIA will still be able to make a successful connection (unless configured to check for it in the authentication profile).	All	The scope of this change is such that if an OU is present in the DN, it will be used, and if it is not, it won't be counted against. As guidance includes usage of the OU in the authentication profile, this has no impact on any claims in the Security Target and merely ensures compatibility with new settings in Aruba gateways.
An issue is resolved in VIA 4.4 where VIA failed to connect with class B (digital badge) certificates in Linux.	Linux	Digital badges were not claimed in the ST and so this change is out of scope of the evaluated configuration.
Resolved an issue where VIA was automatically reconnecting and blocking traffic after reboot when in a trusted network.	Windows	This change does not impact the evaluated configuration.
Improvements were made to how VIA 4.4 manages GRE traffic destined for the L3 adapter which resolves an issue where VIA could discard GRE packet, allowing the VIA client to drop the connection.	Windows	Tunnel mode is the only approved mode in the evaluated configuration. GRE outside the scope of the evaluated configuration.
Non-TOE Platform Fixes		
An issue was resolved where users were unable to connect using 3DES in 4.4, and VIA for iOS and VIA for macOS are now able to connect using 3DES encryption	iOS macOS	In the evaluated configuration, the VIA client does not have 3DES enabled. In addition, neither iOS nor macOS is claimed as an evaluated platform.

Resolved an issue with releases prior to VIA4.4 where VIA could reconnect after Maximum session time is reached if auto connect is enabled.	iOS	iOS is not claimed as an evaluated platform.
Improvements were made to how VIA manages source address selection.	macOS	macOS is not claimed as an evaluated platform. Additionally, it does not affect any SFRs and is outside the scope of the TOE.
VIA 4.4 now shows the certificate details in the VIA app UI. Certificate details were not displayed in the VIA app in VIA 4.3	iOS	iOS is not claimed as an evaluated platform. In addition, this is a UI feature enhancement. It is outside of the scope of the evaluation.

Regression Testing:
Aruba has performed regression testing on VIA 4.4 and all platforms in the ST have been subject to testing. This regression testing is conducted by the dedicated Quality Assurance team for VIA and comprises a subset of their functional test battery for the product. As part of all product releases, Aruba products go through regression testing in accordance with the Common Criteria requirements to ensure no previous functionality has been impacted.

NIST CAVP Certificates:
Not Applicable. No changes were made to the operational environment or to the cryptographic functions claimed in the ST.

Vulnerability Analysis:
A new search was performed for vulnerabilities from the time of the original evaluation (8 August 2022) to 20 January 2023. The search was conducted against the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search) and used the same terms as the original evaluation:

- Aruba
- Arubanetworks
- Aruba VIA
- Virtual Internet Client
- Aruba Virtual Intranet Access
- IPsec VPN Client

The vulnerability search returned 106 results. The only result relating to Aruba VIA 4.x was CVE-2022-23678. However, this vulnerability only affected versions of VIA prior to 4.3. Version 4.4 is unaffected.

Conclusion:

The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims. The updates described above were made to support the new TOE minor version number.

Regression testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, the platforms did not change and there were no necessary alterations to the NIST cryptographic certificates. Therefore, CCEVS agrees that the original assurance is maintained for the product.