ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

NUBO CLIENT VERSION 3.3.1

Nubo Client Version 3.3.1

Maintenance Report Number: CCEVS-VR-VID11380-2026
Date of Activity: 13 February 2026
References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, September 12, 2016
- *Nubo Client Impact Analysis Report for Common Criteria Assurance Maintenance*, Version 0.5, February 6, 2026
- *Nubo Client Version 3.3.1 Security Target*, Version 1.22, February 6, 2026
- *Nubo Client Version 3.3 Guidance Document*, November 2025
- *Vulnerability Assessment for Nubo Client v3.3.1*, version 0.6, February 10, 2026
- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 [APP_PP]
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, March 1, 2019 [PKG_TLS]

Assurance Continuity Maintenance Report:

Acumen Security submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on November 18, 2025 on behalf of Nubo Software LTD. 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 CC Administrator Guide, the Vulnerability Assessment (VA), and the Impact Analysis Report (IAR). The ST, CC Admin Guide and VA were updated.

Documentation updated:

Previous CC Evaluation Evidence	Evidence Change Summary
Security Target: *Nubo Client v3.2 Security Target*, Version 1.18, December 15, 2023	**Maintained Security Target:** See references above. • ST title changed from "Nubo Client v3.2 Security Target" to "Nubo Client v3.3.1 Security Target". • ST version changed from "1.18" to "1.22". • ST date changed from "December 15, 2023" to "February 6, 2026". • TOE version number changed from 3.2 to 3.3.1 • Third-party libraries listed in "FPT_LIB_EXT.1" have been updated to match with the v3.3.1 Software Bill of Materials (SBOM) and includes the latest versions of the packages. • Section 1.4: Updated the identification of the cryptographic library from "BoringSSL" (Native engine) to "Conscrypt" (Java Cryptography Provider): The update from BoringSSL to Conscrypt reflects an alignment with the Android Java Cryptography Architecture (JCA). Conscrypt is the library that exposes security functions to the application layer; it serves as the primary interface for TLS/SSL and cryptographic operations within the evaluated software. While BoringSSL remains the underlying native engine providing the mathematical primitives, naming Conscrypt provides a more complete description of the cryptographic boundary, encompassing both the native execution (BoringSSL) and the Java Native Interface (JNI) layer that manages key handles and session state. This change ensures the ST accurately reflects the library as it is called by the application, with no loss of security functionality or reliance on the underlying BoringSSL core.

Previous CC Evaluation Evidence	Evidence Change Summary
Design Documentation: See Security Target and Guidance	Minor changes required
Guidance Documentation: *Nubo Client Version 3.3 Guidance Document*, 15 December 2023	**Maintained Guidance Documentation:** See references above. • Title and date updated. • TOE version number changed from 3.2 to 3.3
Lifecycle: None	No changes required.
Testing: Vendor regression testing	Vendor regression test results were produced and found consistent with the previous test results. Nubo performs extensive regression and unit testing for every release.
Vulnerability Assessment: *Vulnerability Assessment for Nubo Client v3.2*, Version 1.3, December 15, 2023	**Maintained Vulnerability Assessment Documentation:** A new search was performed for public vulnerabilities on February 10, 2026. The results of the vulnerability assessment were included in the VA. No new TOE vulnerabilities were detected.

Changes to the TOE:

The TOE changes consist of:

- Updates to Nubo Client software from version 3.2 to version 3.3.1. The updates include new non-security relevant features and enhancements.

Major Changes

None.

Minor Changes

Category	Number of Changes	Applicability to New Firmware Versions
Feature Enhancements	10	The feature enhancements from 3.2 to 3.3.1 were enhancement updates that do not affect TOE boundary or evaluated security functionality and included: updates to libraries; improved notification reliability; orientation/rotation fixes; synchronization of critical camera API calls; improved screen area detection; routine maintenance and Android compatibility updates; and refinement of application's handling of device orientation changes.
New Features	3	New features introduced between versions 3.2 and 3.3.1 do not affect TOE boundary or evaluated security functionality and included: adding property tags to hide or disable specific Settings items; adding configurable session timeouts and custom preferences; adding stability refinements for newer Android releases; and fixing product functionality.

Changes to the TOE Operational Environment:

Major Changes
None.

Minor Changes
None.

Equivalency:

The security functionality of Nubo Client remains the same as the original evaluation. The hardware platform is unchanged from the previous maintained version.

NIST CAVP Certificates:

Nubo Client 3.3.1 did not introduce any new cryptographic functionality; therefore, new CAVP certificates were not required.

Vulnerability Analysis:

An updated vulnerability analysis was performed on February 6, 2026, using the original plus additional search terms and the original databases. No applicable vulnerabilities were found.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

CCEVS reviewed the documentation updates and found them to be minor in nature. In particular, the change in the identified cryptographic library from "BoringSSL" to "Conscrypt" in the Security Target is a documentation change to provide additional clarification on how cryptographic operations are invoked. Conscrypt is the library that actually exposes the security functions to the application layer. Both BoringSSL and Conscrypt are already present in the TOE.

The new features and other updates made to Nubo Client from v3.2 through v3.2.82, v3.2.92, v3.2.106, v3.2.122, v3.3, and v3.3.1 do not affect the security claims in the Nubo Client Security Target. These updates result in no changes to SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment and therefore constitute a minor change. The Security Target and the Common Criteria Evaluation Guidance Document are updated to reflect the firmware minor version update.

Regression testing was done and was considered adequate based on the scale and types of changes made. The laboratory also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, Nubo Client v3.3.1 did not introduce any new cryptographic functionality; therefore, new CAVP certificates were not required. CCEVS agrees that the original assurance is maintained for the product.