ASSURANCE CONTINUITY MAINTENANCE REPORT FOR HYPORI HALO CLIENT (ANDROID) 4.3

Maintenance Update of Hypori Halo Client (Android) 4.3.0 to 4.3.25

Maintenance Report Number: CCEVS-VR-VID11423-2026

Date of Activity: 19 February 2026

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;

Hypori Halo Client (Android) 4.3

Impact Analysis Report, Version 1.0, February 2026

Documentation Updated: The original documentation has been updated to the following:

Security Target: Hypori Halo Client (Android) 4.3 Security Target, Version 1.0, February 18, 2026

Changes in the Security Target are:

- Updated document date on cover page
- Copyright date updated
- Section 1.1 – updated ST date
- Section 5.2.2.2 – updated FDP_DEC_EXT.1.1 to specify “Biometrics” instead of “Fingerprint scanner”, as the updated TOE can support additional biometric mechanisms provided by the Android platform (e.g., facial recognition)
- Section 5.2.6.4 – updated version numbers of some third-party libraries listed in FPT_LIB_EXT.1
- Section 6.6.4 – updated version numbers of some third-party libraries to be consistent with updated libraries listed in FPT_LIB_EXT.1
- Section 9 – added Android APIs invoked by the TOE in support of updated platform-provided camera subsystem

Guidance Documentation: Changes were made to the guidance documentation, including:

- Updated product name on cover page and throughout document.
- Removed references to Hypori Windows client, as this is not covered in the Assurance Maintenance submission.
- Section 4.1 – added description of Android “View network connections” permission.
- Section 5 – removed example figure of default client policy settings on Android client.
- Section 7 – updated figures for updated Hypori look and feel.

Assurance Continuity Maintenance Report

On behalf of the vendor, the CCTL, Leidos submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the CCEVS for approval in December 2025. Addressing some of the comments from the validation team, an updated version of the IAR was submitted on February 18, 2026. The IAR is intended to satisfy the 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 validated TOE, the evidence updated because of the changes, and the security impact of the changes.

The updates include re-branding following a change of ownership from "Hypori Halo Client" to "Hypori Client", new non-security relevant features and enhancements, and bug fixes. The updated public vulnerability search was performed on Feb 18, 2026. All potential vulnerabilities were determined to be mitigated/fixed or not applicable to the evaluated configuration. No residual vulnerabilities were identified.

Summary description of Changes

For this Assurance Continuity, the changes consist of updates to Hypori Client (Android) software from version 4.3.0 to version 4.3.25. The updates include re-branding following a change of ownership from "Hypori Halo Client" to "Hypori Client", new non-security relevant features and enhancements, and bug fixes.

The changes described in this document constitute all changes made to the Hypori Client (Android) 4.3 TOE since the previous Common Criteria evaluation (CCEVS-VR-VID11423-2024). The new features and other updates made do not affect the security claims in the Hypori Halo Client (Android) Security Target.

These updates result in no changes to Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment. The following changes have been made to SFRs:

- Updating the version numbers of some third-party libraries listed in FPT_LIB_EXT.1.1, where libraries have been updated to address published security vulnerabilities
- Replacing "[Fingerprint scanner]" with "[Biometrics]" in FDP_DEC_EXT.1.1, as the updated TOE can support additional biometric mechanisms provided by the Android platform (e.g., facial recognition). This change did not require any change in the TSS, as the evaluated TOE supports the USE_BIOMETRIC permission. Regression testing was done to verify that the biometric mechanism wouldn't break any of the legacy mechanisms under authentication subsystem.

As such, the updates to the TOE constitute a **minor** change.

Following is a summary of changes, describing the origin, type, impact, and rationale for each impact determination.

Change Origin	Change Summary	Change Type	Impact Analysis
New_Feature	Introduced a modernized camera subsystem for in-app camera operations.	Rendering/Codec	Minor – improved usability and performance without affecting evaluated security functionality.
Update	Improved support for new and extended disconnect policies.	Policy/Configuration	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Added helper messaging to improve WSA deployment performance.	Network/Protocol	Minor – improved usability without affecting evaluated security functionality.
Update	Updated disconnect policy display to reflect the active configuration.	UI/UX	Minor – improved reliability without affecting security functionality.
Third_Party_Library_Change	Updated obfuscation and anti-tampering library.	Third-Party Library	Minor – updated existing capability without affecting evaluated security functionality.
New_Feature	Added cancellation warning during account creation to prevent unintended enrollment restart.	UI/UX	Minor – improved usability without affecting evaluated security functionality.
Update	Enhanced crash detection mechanisms.	Logging/Telemetry	Minor – improved usability without affecting evaluated security functionality.

Update	Further updated the camera subsystem for reliability improvements.	Rendering/Codec	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Implemented a structured error-handling framework for informational, warning, and error reporting.	Logging/Telemetry	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Added compatibility with Android 14 devices.	Platform/Environment	Minor – improved usability without affecting evaluated security functionality.
Update	Raised Play Store minimum supported Android version to Android 11.	Platform/Environment	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Enabled device biometrics and PIN/passcode authentication for Virtual Device access.	Authentication	Minor – improved usability and updated existing capability without affecting evaluated security functionality.
Update	Modified biometric enrollment prompt to allow PIN/password as the default authentication option.	Authentication	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Enabled the application to remain active in the background.	Platform/Environment	Minor – improved usability without affecting evaluated security functionality.
Update	Prevented automatic notification enablement	UI/UX	Minor – improved usability without

	during account rename operations.		affecting evaluated security functionality.
Update	Removed user codec selection and standardized VP8 as the default codec behavior.	Rendering/Codec	Minor – improved usability without affecting evaluated security functionality.
Update	Adjusted connection channel timeout parameters.	Network/Protocol	Minor – improved reliability without affecting evaluated security functionality.
New_Feature	Expanded supported certificate types during account setup.	Cryptography	Minor – improved usability and reliability without affecting evaluated security functionality.
Update	Updated app permissions.	Policy/Configuration	Minor – improved usability and reliability without affecting evaluated security functionality.
New_Feature	Updated application branding to reflect new corporate look.	UI/UX	Minor – improved usability and reliability without affecting evaluated security functionality.
Update	Improved reliability on Android 15 devices.	Platform/Environment	Minor – improved usability and reliability without affecting evaluated security functionality.
Update	Refined biometric-related error messaging.	Authentication	Minor – improved usability without affecting evaluated security functionality.

Update	Modified background audio behavior to include microphone use.	Network/Protocol	Minor – improved usability without affecting evaluated security functionality.
Third_Party_Library_Change	Updated third-party libraries to remediate identified vulnerabilities.	Dependency Update	Minor – updated existing capability without affecting evaluated security functionality.
New_Feature	Extended biometric authentication to Virtual Workspace lock screen and applications.	Authentication	Minor – added capability without affecting evaluated security functionality.
Update	Raised minimum supported Android version to Android 12.	Platform/Environment	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Added support for Hypori Flex seamless migration.	Network/Protocol	Minor – improved usability without affecting evaluated security functionality.
Update	Updated notification behavior and simplified badges.	UI/UX	Minor – improved usability without affecting evaluated security functionality.
Update	Updated touch event capture implementation.	UI/UX	Minor – improved usability without affecting evaluated security functionality.
Update	Added support for Android 15 SDK.	Platform/Environment	Minor – improved usability without affecting evaluated security functionality.

New_Feature	Enabled GPS-based apps to continue running in background or when device is locked.	Platform/Environment	Minor – improved usability and performance without affecting evaluated security functionality.
Update	Improved connection retry logic for Flex environments.	Network/Protocol	Minor – improved usability and performance without affecting evaluated security functionality.
New_Feature	Added pre-start feature to reduce connection time.	Performance	Minor – improved usability and performance without affecting evaluated security functionality.
Update	Updated camera for improved quality and reliability over VPN connections.	Rendering/Codec	Minor – improved usability and performance without affecting evaluated security functionality.
Update	Split audio input and output into separate network connections.	Network/Protocol	Minor – improved reliability without affecting evaluated security functionality.
Update	Updated keyboard alignment to reduce overtap issues.	UI/UX	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Added support for 16KB NDK page size.	Platform/Environment	Minor – added capability without affecting evaluated security functionality.
New_Feature	Added support for	Platform/Environme	Minor – added capability without affecting

	foldable devices.	nt	evaluated security functionality.
Update	Improved connection state monitoring.	Network/Protocol	Minor – improved usability without affecting evaluated security functionality.
New_Feature	Added support for OIDC authentication mechanisms.	Authentication	Minor – improved usability and updated existing capability without affecting evaluated security functionality.

Regression Test Summary

The CCTL reported that Vendor regression test results were produced and found consistent with the previous test results. Hypori performed extensive regression testing for every release of Hypori Client (Android). Hypori's regression testing comprises execution of automation test suites and additional manual testing, focused on both functionality and security.

Vulnerability Analysis Summary

A public search for new vulnerabilities that might affect the TOE since the evaluation was completed was performed. The evaluation team performed final searches on 18 February 2026. The search did not identify any new potential vulnerability that affects the updated TOE. In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version update.

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.