CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

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

Maintenance Update of Hypori Halo Client (iOS) 4.3.0 to 4.3.75

Maintenance Report Number: CCEVS-VR-VID11425-2026

Date of Activity: 05 March 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 (iOS) 4.3 Impact Analysis Report, Version 1.0, 03 March 2026.

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

Security Target: Hypori Halo Client (iOS) 4.3 Security Target, Version 1.0, February 24, 2026

Changes in the Security Target are:

- Updated document date and Copyright date on cover page
- Section 1.1 – updated ST date
- Section 2.4 – updated title of user guide to correctly reflect document title
- Section 5.2.2.2 – replaced "[Fingerprint scanner"] with "[Biometrics]" in FDP_DEC_EXT.1.1 to reflect broader product support for platform-provided biometric mechanisms rather than just a fingerprint scanner.
- Section 5.2.6.4 – updated list of third-party libraries in FPT_LIB_EXT.1.1
- Section 6.6.4 – updated list of third-party libraries consistent with updated statement of FPT_LIB_EXT.1
- Section 9 – added UIKeyCommand to list of iOS APIs used by the TOE. This API was introduced into the TOE in Release 4.3.4

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 26, 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", some changes to third-party libraries, new non-security relevant features and enhancements, and bug fixes. The updated public vulnerability search was performed on Feb 26, 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 (iOS) software from version 4.3.0 to version 4.3.75. 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 (iOS) 4.3 TOE since the previous Common Criteria evaluation (CCEVS-VR-VID11425-2024). The new features and other updates made do not affect the security claims in the Hypori Halo Client (iOS) 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:

- Update the list of third-party libraries in FPT_LIB_EXT.1.1, which include
  - Some libraries listed in the original evaluated ST have been removed as they are indirect dependencies (i.e., dependencies of dependencies) and should not have been included in the original ST: *ios-openssl, swift-atomics, swift-collections, swift-log, swift-nio, swift-nio-extras, swift-nio-http2, swift-nio-ssl, swift-nio-transport-services, SwiftProtobuf.*
  - *PLCrashReporter* library has been removed as it is no longer used by the TOE.
  - Replaced "spice-qtk" with "spice-gtk"—this was a typographic error in the ST, the library itself is unchanged.
  - Some new libraries have been added in the TOE to support new capabilities: *AppAuth* (new OIDC authentication functionality), *firebase-ios-sdk* (to enable application crash monitoring replacing *PLCrashReporter*), *libyuv*, *libvpx* (new feature for VP8 video encoding, replacing existing H264 encoding), and *CommonIOS* (supporting internal refactoring efforts).

- Replace "[Fingerprint scanner]" with "[Biometrics]" in FDP_DEC_EXT.1.1, as the updated TOE can support additional biometric mechanisms provided by the iOS platform (e.g., facial recognition). This change did not require any change in the TSS, as the evaluated

TOE supports the FaceID/TouchID permission.

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
Update	Updated the display stream to optimize application launches.	Performance	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Updated the obfuscation and anti-tampering library.	Third-Party Library	Minor - Updated existing capability without affecting evaluated security functionality.
New Feature	Introduced a VP8 codec for the Virtual Workspace display.	Rendering/ Codec	Minor - Improved usability without affecting evaluated security functionality.
Update	Updated API declarations to satisfy new App Store requirements.	Network/ Protocol	Minor - Improved usability without affecting evaluated security functionality.
New Feature	Added a codec selection switch for bandwidth selection.	UI/UX	Minor - Improved usability without affecting evaluated security functionality.
New Feature	Introduced warnings when users attempt to cancel account creation.	UI/UX	Minor - Improved usability without affecting evaluated security functionality.
Update	Removed a private API.	Refactoring	Minor - Improved security without affecting evaluated security functionality.
Update	Optimized the size of audio data sent.	Performance	Minor - Improved performance without affecting evaluated security functionality.
Update	Set the default codec to VP8.	Rendering/ Codec	Minor - Improved usability without affecting evaluated security functionality.
Update	Modified secondary authentication to stop prompting for username unnecessarily.	Authentication	Minor - Improved usability and performance without affecting evaluated security functionality.
New Feature	Introduced a higher performance VP8 codec for camera images and video.	Rendering/ Codec	Minor - Improved usability and performance and updated existing capability without affecting evaluated security functionality.
Update	Updated the camera subsystem to support VP8.	Rendering/ Codec	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
New Feature	Added an immersive full screen mode for the Virtual	UI/UX	Minor - Improved usability and updated existing capability without affecting

	Device.		evaluated security functionality.
New Feature	Added support for device biometrics and passcode authentication to the Virtual Device.	Authentication	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Updated the app notification function to allow multiple push notification paths.	Network/ Protocol	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
New Feature	Enabled audio playback while the app is in the background.	Platform/ Environment	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Updated the upgrade prompt to support migration to a new app package name.	UI/UX	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
New Feature	Added capability to send logs to Hypori Support.	Logging/ Telemetry	Minor - Improved usability and reliability and updated existing capability without affecting evaluated security functionality.
Update	Updated network handover function to prioritize stable connections.	Network/ Protocol	Minor - Improved usability and reliability and updated existing capability without affecting evaluated security functionality.
Update	Updated memory management mechanisms.	Refactoring	Minor - Improved reliability and updated existing capability without affecting evaluated security functionality.
New Feature	Added prompts to assist users with biometric setup.	Authentication	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Improved biometric authentication features and error handling.	Authentication	Minor - Improved reliability and updated existing capability without affecting evaluated security functionality.
Update	Updated touch event handling for improved gesture recognition.	UI/UX	Minor - Improved usability and reliability and updated existing capability without affecting evaluated security functionality.
Update	Improved keyboard management functions.	UI/UX	Minor - Improved usability and reliability and updated existing capability without affecting evaluated security functionality.
Update	Updated connection channel timeouts.	Network/ Protocol	Minor - Improved usability and reliability and updated existing capability without affecting evaluated security functionality.

Update	Updated capturing of screen touches for gesture reliability.	UI/UX	Minor - Improved usability and reliability and updated existing capability without affecting evaluated security functionality.
Update	Further improved biometric authentication user experience.	Authentication	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Improved connectivity reliability.	Network/ Protocol	Minor - Improved reliability without affecting evaluated security functionality.
New Feature	Introduced new app branding.	UI/UX	Minor - Improved usability without affecting evaluated security functionality.
New Feature	Added support for background disconnect policy.	Policy/ Configuration	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Updated the send log feature to include communications errors.	Logging/ Telemetry	Minor - Updated existing capability without affecting evaluated security functionality.
New Feature	Added upgrade reminder for app migration.	UI/UX	Minor - Improved usability without affecting evaluated security functionality.
Update	Updated multiple library dependencies.	Dependency Update	Minor - Improved usability and reliability without affecting evaluated security functionality.
New Feature	Changed the display engine to render using Metal.	Rendering/ Codec	Minor - Improved performance and reliability without affecting evaluated security functionality.
Update	Improved logging to capture more information about crashes.	Logging/ Telemetry	Minor - Improved usability and reliability without affecting evaluated security functionality.
New Feature	Enhanced app security from prying eyes by enabling screen recording prevention.	Other	Minor - Improved reliability by strengthening data-at-rest and data-in-transit posture without affecting evaluated security functionality.
Update	Set the new rendering feature as the default option.	Rendering/ Codec	Minor - Improved usability without affecting evaluated security functionality.
New Feature	Added biometric authentication support for the Virtual Workspace lock screen and apps.	Authentication	Minor - Improved usability and updated existing capability without affecting evaluated security functionality.
Update	Removed the “New” moniker from the app name and icon.	UI/UX	Minor - Improved usability 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 (iOS). Hypori's regression testing comprises execution of automation test suites and additional manual testing, focused on both functionality and security. Tests are executed monthly, and new vulnerabilities are resolved as soon as possible in the next Hypori release cycle. Hypori also employs the zShield application to prevent tampering and reverse engineering, which is upgraded monthly to combat vulnerabilities and new exploits. Additionally, Hypori engages in at least 2 manual penetration tests per year.

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.