Qubic Wallet

Mobile Application Security Assessment

Kudelski Security – EMEA Offensive Security Team

Contact us at offensive-services@kudelskisecurity.com

Kudelski Security – Offensive Security Team, the Cyber Security Division of the Kudelski Group, has been mandated by Qubic to conduct a security assessment in the form of penetration tests of the Qubic Wallet mobile application.

The mobile application penetration tests were conducted between August 18, 2025, and August 26, 2025, covering both the Android and iOS versions of the Qubic wallet application.

A retest was subsequently performed on November 5 and November 11, 2025, to verify the remediation of previously identified issues and to confirm that the implemented fixes did not introduce any regressions.

The assessment focused on the following objectives:

1. Help Qubic better understand its current risks and overall security posture across the Android and iOS mobile applications.
2. Provide a professional opinion on the maturity, adequacy, and effectiveness of the security measures in place.
3. Identify potential security weaknesses and provide evidence-based recommendations for improvement based on the results of the penetration testing activities.

Scope

The engagement consisted of a white-box penetration test of the Qubic Wallet mobile applications listed above, assessing client-side functionality, local storage, network communications, authentication, cryptographic handling, and common mobile platform attack vectors.

Asset	Version
Qubic Wallet Android mobile application	Qubic Waller v2.0.1 (72)
Qubic Wallet iOS mobile application	Qubic Waller v2.0.1 (73)

Published on 22.05.2024

FINDINGS

The following points summarize the main findings from the assessment, including notable security strengths and identified weaknesses.

Strengths

Secrets remain on device: Sensitive user data—such as wallet passphrases and private keys are never transmitted to backend servers and are securely stored on-device using platform-specific features like Keychain and Keystore, ensuring strong client-side privacy.

No critical vulnerabilities identified: Both iOS and Android applications follow secure coding practices. The assessment did not uncover any critical vulnerabilities, reflecting a strong overall security posture.

Vulnerabilities

MOB1 – Improper authentication implementation

Severity: LOW | Status: OPEN

The wallet authentication mechanism can be bypassed on devices that are rooted or jailbroken. By dynamically hooking authentication functions, a local attacker with full control of such a device could access wallet content without providing the correct password or biometric credentials.

This scenario remains highly constrained as it requires prior device compromise. The application implements root/jailbreak detection, which significantly raises the difficulty for non-technical attackers. However, such checks can be bypassed with time and expertise.

MOB2 – Backup of sensitive wallet data on iOS

Severity: LOW | Status: FIXED

In earlier versions, encrypted wallet data stored in the iOS *Documents* directory and managed through the Keychain could potentially be included in iCloud backups. This exposure could have allowed recovery of encrypted wallet data through a compromised backup.

The updated implementation now ensures that sensitive Keychain items cannot be restored on another device, while remaining accessible on the same device as intended. The configuration uses *KeychainAccessibility.unlocked*, chosen for its balance between usability and security after reviewing industry behavior across leading crypto wallets.

The update also migrates existing Keychain entries when users first run the new version, ensuring a consistent and secure upgrade path.

MOB3 – Vault encryption vulnerable to offline attacks

Severity: LOW | Status: FIXED

The wallet backup vault feature encrypts exported data using AES-256-GCM, with the key derived from the user's password via PBKDF2 (100,000 iterations). This configuration provided limited resistance to modern offline brute-force attacks if users chose weak passwords.

The current implementation enforces a minimum password length of 12 characters for all export operations, significantly improving resistance to offline guessing.

Published on 22.05.2024

Further evaluation of stronger key-derivation parameters (e.g., Argon2id or higher PBKDF2 iteration counts) is ongoing, as such changes would affect interoperability with related products that import the same backup format.

MOB4 – Unprotected screenshot of seed phrase

Severity: LOW | Status: FIXED

Screenshot protection was inconsistently applied in prior versions, allowing sensitive seed phrases to be captured during wallet creation or import. This risked unintentional disclosure through stored screenshots or malicious screen-capture apps.

The protection is now enforced consistently, including within the "*Create New Account*" and "*Import Private Seed*" workflows, ensuring that private keys and seed phrases cannot be captured visually on any sensitive screen.

MOB5 – Unrestricted URL access in WebView

Severity: LOW | Status: OPEN

The "Explore" WebView component allows users to load arbitrary URLs. Although the WebView operates in a sandbox and currently exposes no native interfaces, unrestricted URL access introduces unnecessary attack surface.

If future updates were to expose JavaScript bridges or other integrations, a malicious or compromised page could potentially attempt code injection or phishing attacks. Restricting the WebView to trusted domains would reduce this risk.

MOB6 – API missing HTTP security headers

Severity: LOW | Status: OPEN

The API endpoint (rpc.qubic.org) was found to lack certain standard HTTP security headers (e.g., Strict-Transport-Security, Content-Security-Policy, X-Frame-Options). While this has minimal direct impact on mobile clients, implementing these headers is considered best practice and improves defense-in-depth for any web-based interactions.

Conclusion

The identified issues were low risk and primarily related to potential improvements in security hardening. Both the Android and iOS applications demonstrate a solid security posture, with no significant vulnerabilities identified. Sensitive user data is securely stored on-device using platform-level encryption features, further protecting user privacy and application integrity.

Published on 22.05.2024