

Case Study: Local Passcode Bypass via Connectivity Interruption

Researcher: Klark Kent Pantalla

Target: ioPay Wallet (Mobile Authentication Layer)

Severity: High (Broken Authentication Logic)

1. Executive Summary Identified a critical authentication bypass in the ioPay mobile application where the local passcode gatekeeper fails to trigger during specific network state transitions. By manipulating the WiFi connectivity state during a failed login attempt, the application bypasses the security layer and grants full access to the wallet dashboard.

2. Environment & Test Parameters

- **Device:** Samsung Galaxy S9+
- **Operating System:** Android 10
- **Application Version:** ioPay v4.7.4

3. Vulnerability Description (Step-by-Step)

1. **Initial State:** Application is locked with a mandatory local passcode.
2. **Trigger:** Attempting multiple incorrect passcode combinations to engage the authentication service.
3. **Manipulation:** Disabling the device WiFi/Network connection while the app is in the "Locked" state.
4. **The Flaw:** Upon returning to the application while offline, the app displays a "No Connection" error but fails to persist the "Locked" state.
5. **The Bypass:** Once the network connection is restored, the application automatically navigates directly to the wallet dashboard, completely skipping the passcode requirement.

4. Security Impact This vulnerability renders the local passcode feature ineffective. An unauthorized user can gain full access to the wallet's private data and transaction capabilities simply by toggling the device's network connection, bypassing the primary line of physical security.

5. Resolution & Remediation

- **Logic Fix:** The application was programmed to require a "Success" callback from the local authentication service before initializing the MainActivity, regardless of connectivity status.
- **Status: Resolved.** The development team implemented **Strict State Enforcement**, ensuring the "Locked" state remains persistent even during network state transitions.
- **Verification:** Post-patch testing on updated builds confirmed that toggling WiFi no longer bypasses the mandatory passcode screen.