Fix Report: User Address Authenticity Verification

1. Reference:

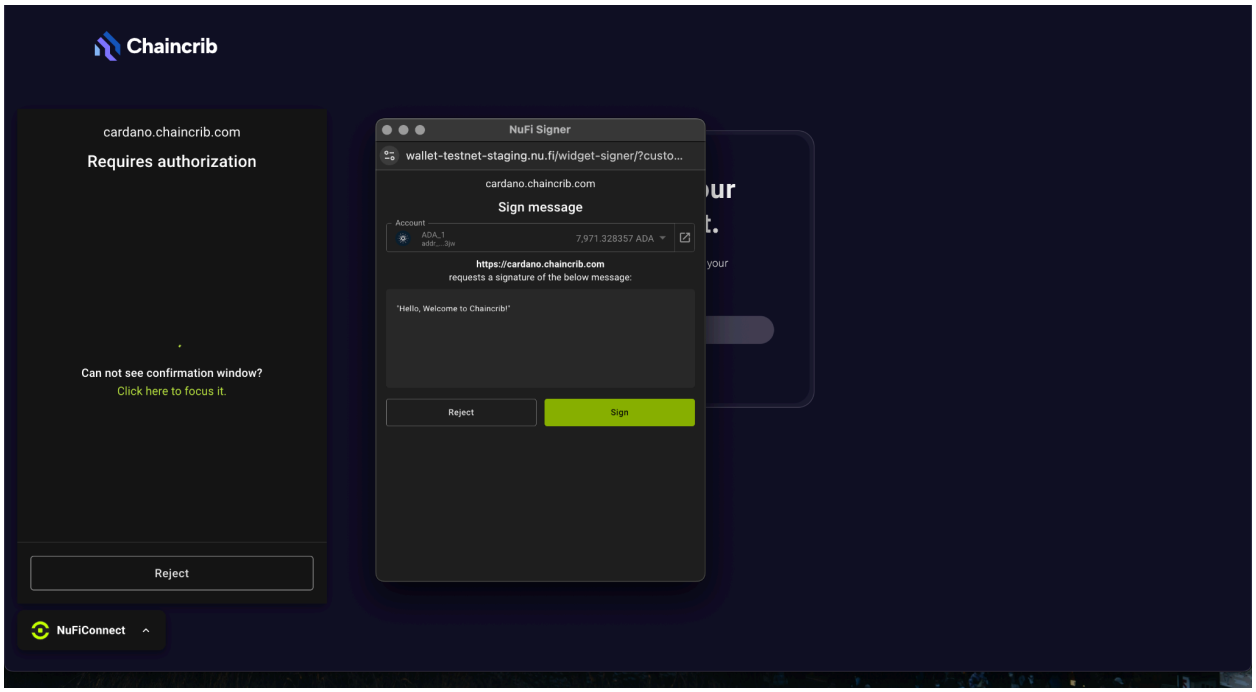
- Signed Transaction Handling: Accuracy of the recipient wallet address

2. Original Vulnerability:

- **Description:** Previously, the application lacked a robust mechanism to verify the authenticity of user-provided addresses. This could have allowed an attacker to impersonate users by submitting false addresses associated with their accounts, bypass certain address-based restrictions, misdirect funds, or sensitive information if the address was used for transactional purposes.
- **Impact:** Potential for unauthorized access, fraudulent activities, or data integrity issues.

3. Implemented Fix:

- **Description:** To address the lack of address authenticity verification, a new security measure has been implemented requiring users to sign a cryptographic message. This signed message can then be verified by the application to confirm that the user in possession of the private key associated with the claimed address is indeed the one interacting with the application.
- **Technical Details:**
    - **Mechanism:** When a user wishes to verify or associate an address, the application now generates a message for the user to sign.
    - **User Action:** The user is prompted to sign this message using their private key associated with the address they are verifying. This is typically done using a supported wallet, which in our case is Nufi.
    - **Verification Process:** The application receives the signed message, the original message, and the user's address. It then compares the signature against the address claimed by the user. If they match, the address is deemed authentic and associated with the user's account.
- **Components Affected:** User registration flow, Wallet connection module



5. Verification Steps (for future audits/testing):

- **Test Case 1: Successful Address Verification**
    4. **Steps:**
        1. Initiate the address verification process by signing via the Nufi wallet.
        2. Sign the prompted message using the correct private key for that address.
        3. Submit the signed message to the application.
    5. **Expected Result:** The application successfully verifies the address and associates it with the user's account.
- **Test Case 2: Invalid Signature/Mismatched Address**
    4. **Steps:**
        1. Initiate the address verification process by signing via the Nufi wallet.
        2. Attempt to submit a signed message that was either signed with a different private key, is corrupted, or does not correspond to the claimed address.
    5. **Expected Result:** The application rejects the verification, indicating an invalid signature or a mismatch, and does not associate the address.