CERTIK

Security Assessment

Internet Money Wallet

CertiK Assessed on Dec 27th, 2023

CertiK Assessed on Dec 27th, 2023

Internet Money Wallet

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Wallet	Extension | Mobile Application	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
TypeScript	Delivered on 12/27/2023	N/A

Vulnerability Summary

6	4	0	1	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed immediately. Users should be cautious when interacting with any application with outstanding critical risks.
2	High	2 Resolved	High risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds, thief of user data, and/or loss control of the application.
3	Medium	1 Resolved, 1 Partially Resolved, 1 Acknowledged	Medium risks may not pose a security risk at a large scale, but they can affect the overall functioning of a platform or be used to target a certain group of users.
1	Low	1 Resolved	Low risks can be any of the above, but on a smaller impact. They generally do not compromise the overall integrity of the project.
0	Informational		Informational errors are often recommendations to improve the configuration or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the application.

TABLE OF CONTENTS | INTERNET MONEY WALLET

SCOPE | INTERNET MONEY WALLET

Source Code	https://gitlab.com/internetmoneyio/wallet/mobile/-/tree/fcc2cd05772622ad233862fc44142a68789abb53
Source Code	https://gitlab.com/internetmoneyio/wallet/chrome/-/tree/7094b5b2deecf64fd0333a8f3af46648d9b2f7f1

APPROACH & METHODS | INTERNET MONEY WALLET

This report has been prepared for Internetmoney to discover issues and vulnerabilities in the application of the Internet Money Wallet project. The Internet Money Wallet is a non-custodial crypto wallet that supports multiple ecosystems.

The pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the OWASP Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

The main objective of the engagement is to test the overall resiliency of the application to various real-world attacks against the application's controls and functions and thereby be able to identify its weaknesses and provide recommendations to fix and improve its overall security posture.

Two members of the CertiK team were involved in completing the engagement, which took place over the course of 3 days in December 2023 and yielded 6 security-relevant findings. The most significant issue is the availability of the wallet and the insecure handling of WalletConnect connection requests.

Other weaknesses were also found and are detailed in the Findings section of the report. We recommend addressing these findings to ensure a high level of security standards and industry practices and to raise the security posture of the application.

FINDINGS | INTERNET MONEY WALLET

6	0	2	3	1	0
Total Findings	Critical	High	Medium	Low	Informational

This report has been prepared to discover issues and vulnerabilities for Internet Money Wallet. Through this security assessment, we have uncovered 6 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous testing process, we discovered the following findings:

ID	Title	Category	Severity	Status
GLOBAL-01	The Client-Side Wallet Becomes Completely Unusable When The Wallet API Is Down.	Denial of Service	High	Resolved
GLOBAL-02	Lack Of "Attestation" Origin Verification During WalletConnect Connection	Security Misconfiguration	High	Resolved
GLOBAL-03	Lack Of Certificate Pinning	Insufficient Cryptography	Medium	Resolved
GLOBAL-06	Screenshot Backgrounding	Information Disclosure	Medium	Acknowledged
GLOBAL-07	Private Key Display Allow Screenshot	Insecure Data Storage	Medium	Partially Resolved
GLOBAL-04	Crash Caused By Invalid Token Import	Denial of Service	Low	Resolved

GLOBAL-01 THE CLIENT-SIDE WALLET BECOMES COMPLETELY UNUSABLE WHEN THE WALLET API IS DOWN.

Category	Severity	Location	Status
Denial of Service	High		Resolved

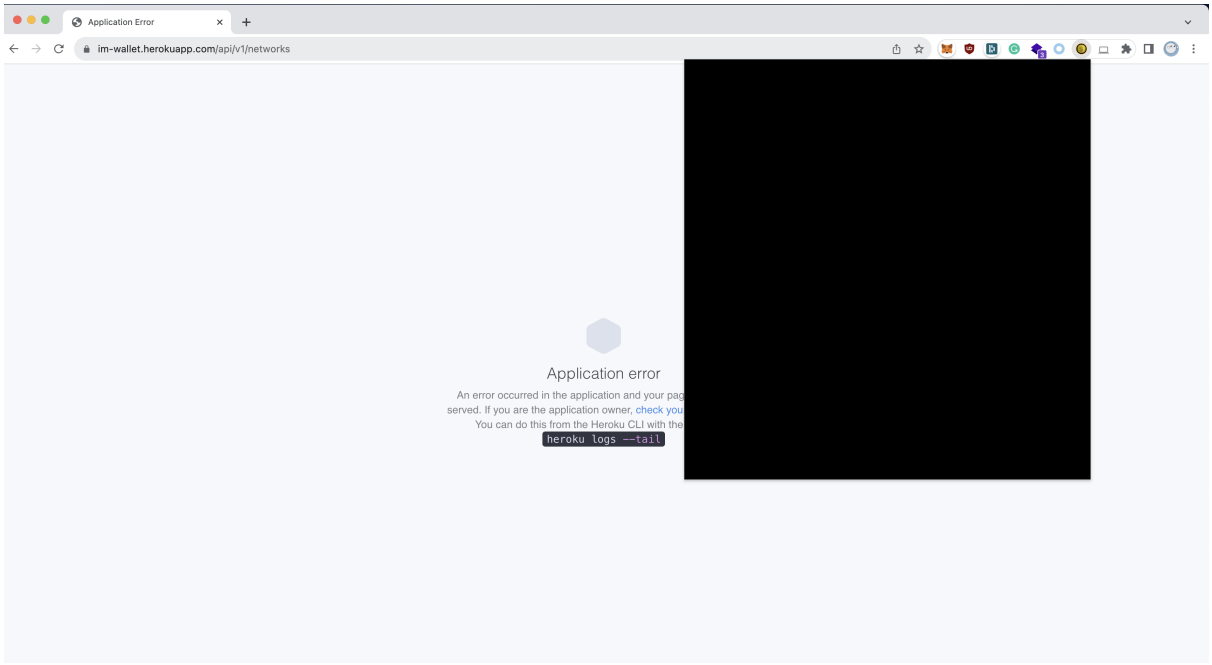
Description

During the security assessment of the Internet Money wallet Chrome extension and mobile app, it was observed that the application becomes entirely nonfunctional when it fails to communicate with server-side APIs. Instead of providing limited functionality or informative error messages to the user, the application displays a blank screen, which severely degrades the user experience.

Impact

The quality of the server-side API appears to be unstable, as indicated in the API's pentest report. When the server-side API encounters issues, it causes the entire wallet to become inoperable, leaving users with a blank screen and no immediate workaround. As a non-custodial, decentralized wallet application, this behavior significantly impacts the wallet's accessibility and reliability. It stops users from viewing their balance, accessing their private keys and seed phrases, or transferring tokens.

Proof of Concept



Recommendation

To mitigate this issue, it is recommended that the wallet application be enhanced to ensure core functionalities remain accessible, even when server-side APIs are down. At a minimum, users should be able to view their balance, export their private key and seed phrase, and initiate token transfers without dependency on server API connectivity.

Alleviation

Fixed in commit 7094b5b2deecf64fd0333a8f3af46648d9b2f7f1.

GLOBAL-02 LACK OF "ATTESTATION" ORIGIN VERIFICATION DURING WALLETCONNECT CONNECTION

Category	Severity	Location	Status
Security Misconfiguration	High		Resolved

Description

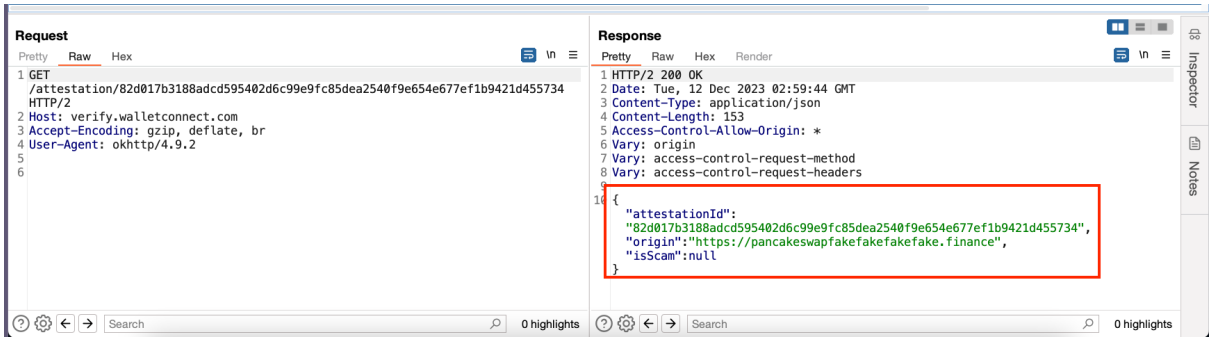
The WalletConnect protocol recently launched a Verify API, which is used to confirm whether the connected origin matches the registered origin on the WalletConnect site. This verification occurs during the connection confirmation in the user's wallet. However, the Internet Money Wallet failed to ensure that the returned origin from the "Attestation"API matches the original origin from the QR code.

Impact

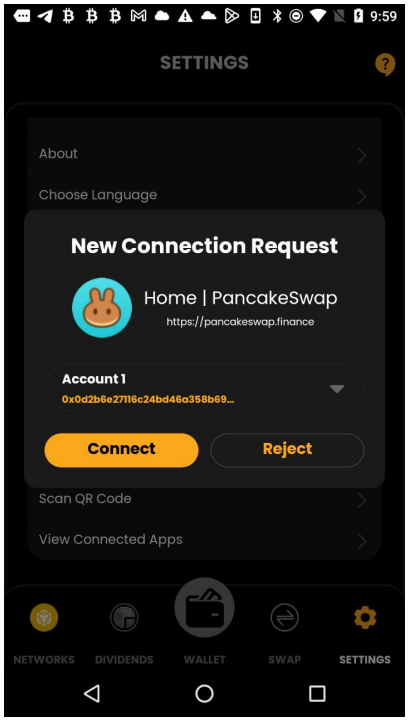
The absence of verification might increase the likelihood of wallet users falling victim to targeted phishing attacks when using WalletConnect to connect with a malicious dApp.

Proof of Concept

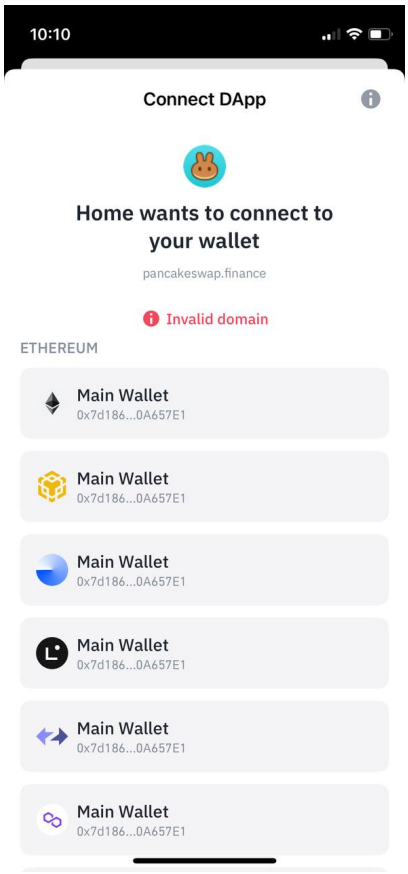
When the user tries to connect to the PancakeSwap DApp using a mobile app, a tampered "attestation" request returns an original that doesn't match the domain the user is trying to connect to. However, the Internet Money Wallet fails to warn the user about the discrepancy. In contrast, when tested with the "Trust Wallet," it displays that the domain is invalid.



Internet Money Wallet's WalletConnect connection pop-up:



When attempting the same attack with the Trust Wallet, it displays a warning stating "invalid domain":



Recommendation

It is recommended that the wallet verifies the returned "origin" value of the "attestation" request against the website the user is attempting to connect to. For more information regarding the Verify API, please refer to:

- https://medium.com/walletconnect/unlocking-the-power-of-verify-api-a-step-by-step-guide-for-wallets-4e939a273d9a
- https://docs.walletconnect.com/web3wallet/verify

Alleviation

Fixed in commit fcc2cd05772622ad233862fc44142a68789abb53.

GLOBAL-03 | LACK OF CERTIFICATE PINNING

Category	Severity	Location	Status
Insufficient Cryptography	Medium	Mobile application: im-wallet.herokuapp.com	Resolved

Description

The application does not implement certificate pinning. Certificate pinning is the act of associating a host with its expected certificate within the application. When the application connects to the host, the stored certificate is compared to the certificate held by the remote host. If the two certificates do not match, the request is dropped. Currently, the application only verifies that the server presents a TLS certificate that is trusted by the Android or iOS trust stores, not validating that the TLS certificate is in fact the one known to be deployed on the servers.

Impact

An attacker can man-in-the-middle traffic between the application and the server, if the attacker is able to install a malicious certificate on the user's Android device and the attacker has a privileged network position. This would allow the attacker to disclose sensitive information or modify requests in transit. Additionally, the application is not protected in the case of a malicious or compromised certificate authority already installed on the mobile device.

Proof of Concept

1. Configure the devices to use Burp Suite as the web proxy.
2. Install the Burp Suite certificate as a system-level trusted certificate in the Android devices.
3. Notice the Burp proxy can intercept the traffic between the client application and the server.

Recommendation

Mobile applications should use certificate pinning to verify the identity of the remote host communicating with the application. Certificate pinning verifies that the client application is connecting to the designated server and not an intermediary attacker.

For more information about certificate pinning and how to implement it in the respective operating systems, see https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning.

Alleviation

Fixed in commit: 14a50a486b584004d2ecdf7e9225026f4f829620

GLOBAL-06 | SCREENSHOT BACKGROUNDING

Category	Severity	Location	Status
Information Disclosure	Medium	View account private key interface	Acknowledged

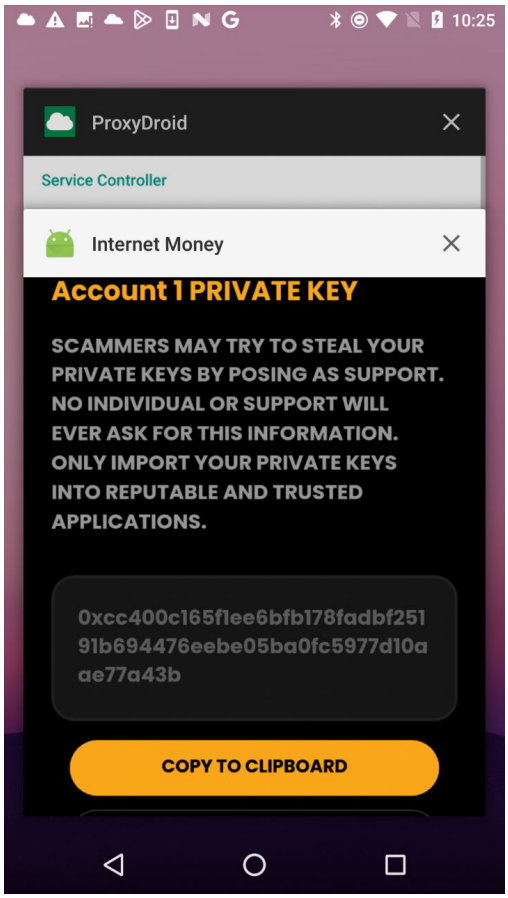
Description

On mobile devices, a screenshot of the current activity is taken when an application goes into the background and displayed for aesthetic purposes when the app returns to the foreground. This feature may pose a security risk. Sensitive data may be exposed if the user backgrounds the application while sensitive data is displayed. A malicious application that is running on the device and able to continuously capture the screen may also expose data.

Impact

An attacker with physical access to the unlocked device or a malicious third party app with access to the auto-generated screenshot of the application can retrieve sensitive information included in the screenshot.

Proof of Concept



Recommendation

It's recommended for the application to add an overlay to hide or obscure the application screen before moving to the background.

For iOS, add an overlay screen before the application goes into the background, and remove the screen when the application goes into the foreground.

For Android, in addition to adding an overlay, this can be done by setting the FLAG_SECURE option. The FLAG_SECURE flag can prevent sensitive information included in the auto-generated screenshot. For more information about the FLAG_SECURE flag, please see https://developer.android.com/reference/android/view/Display#FLAG_SECURE and https://stackoverflow.com/questions/9822076/how-do-i-prevent-android-taking-a-screenshot-when-my-app-goes-to-the-background

Alleviation

[Internet Money team]: This is a relatively low risk threat due to the requirement for a malicious actor to either have physical access to the device or for the user to have installed malicious software with the ability to view screen recordings. Although we have implemented the feature to hide information from the background screenshot on iOS, doing so on Android requires setting the FLAG_SECURE flag to prevent screenshots entirely. In our response to GLOBAL-07, we explain why we have decided not to set the FLAG_SECURE flag. Due to that limitation, we cannot hide this information from the background screenshot on Android.

GLOBAL-07 | PRIVATE KEY DISPLAY ALLOW SCREENSHOT

Category	Severity	Location	Status
Insecure Data Storage	Medium		Partially Resolved

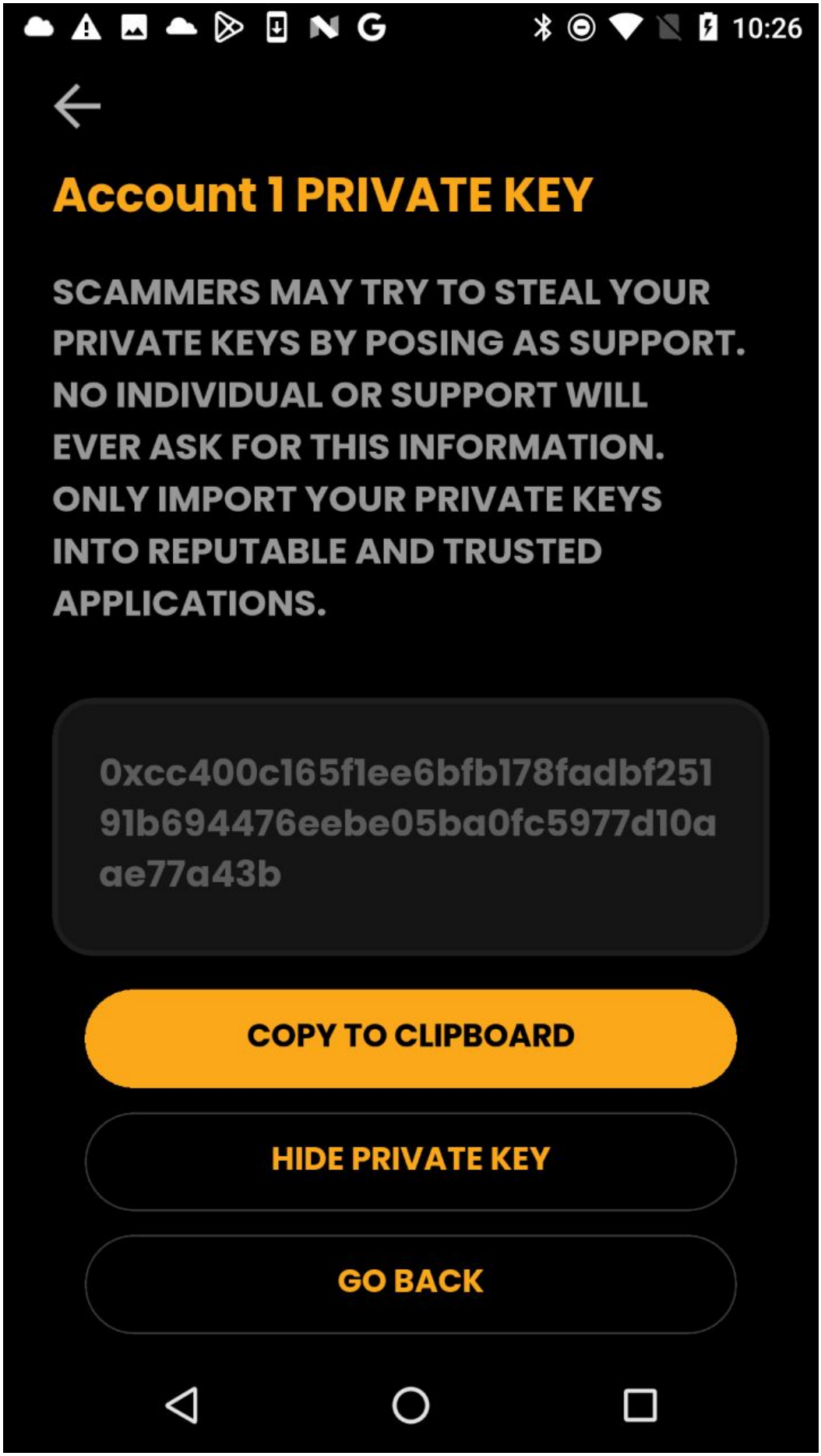
Description

The private key can be used to recover a wallet account. Obtaining the Private key can potentially allow the attacker to gain full control of the wallet. The application neither has a mechanism in place to stop a user from taking a screenshot of the displayed wallet secrets nor displays a warning to remind the user of the risk of taking a screenshot.

Impact

Third party apps with "READ_EXTERNAL_STORAGE" permission on an Android device or apps with all photo access on an iPhone can read screenshots on the device. Third party apps can retrieve the mnemonic if the mnemonic is included in a screenshot taken by the user.

Proof of Concept


10:26
Account 1 PRIVATE KEY
SCAMMERS MAY TRY TO STEAL YOUR PRIVATE KEYS BY POSING AS SUPPORT. NO INDIVIDUAL OR SUPPORT WILL EVER ASK FOR THIS INFORMATION. ONLY IMPORT YOUR PRIVATE KEYS INTO REPUTABLE AND TRUSTED APPLICATIONS.
0xcc400c165f1ee6bfb178fadbf25191b694476eebe05ba0fc5977d10aae77a43b
COPY TO CLIPBOARD
HIDE PRIVATE KEY
GO BACK

Recommendation

Screen capture can be prevented by setting the FLAG_SECURE option. The FLAG_SECURE flag can prevent user and malicious third-party apps from recording the mnemonic screens and taking screenshots of sensitive information. For more information about the FLAG_SECURE flag, please see “https://developer.android.com/reference/android/view/Display#FLAG_SECURE”

iOS

There isn't a built-in solution on iOS to prevent the user from taking the screenshot. It's recommended adding a warning to remind a user not to take screenshots when viewing their wallet secrets.

Alleviation

[Internet Money team]: The risk of this item is relatively quite low, as it requires the user themselves to take a screenshot of their private key or seed phrase and for an attacker to have either physical access to the unlocked device or a malicious app with the correct permissions installed on the user’s device. The Internet Money team believes strongly in strengthening users’ financial freedom. Some users intentionally choose to screenshot their seed phrase or private keys as part of their backup process. While this is not generally the recommended approach, we do not believe it is our position to prevent a user from doing what they choose with their own keys. Instead, we have implemented an addition to our warning text on these pages. Users are advised that capturing a screenshot of their seed phrase or private keys is not recommended, but they are permitted to do so.

GLOBAL-04 | CRASH CAUSED BY INVALID TOKEN IMPORT

Category	Severity	Location	Status
Denial of Service	Low		Resolved

Description

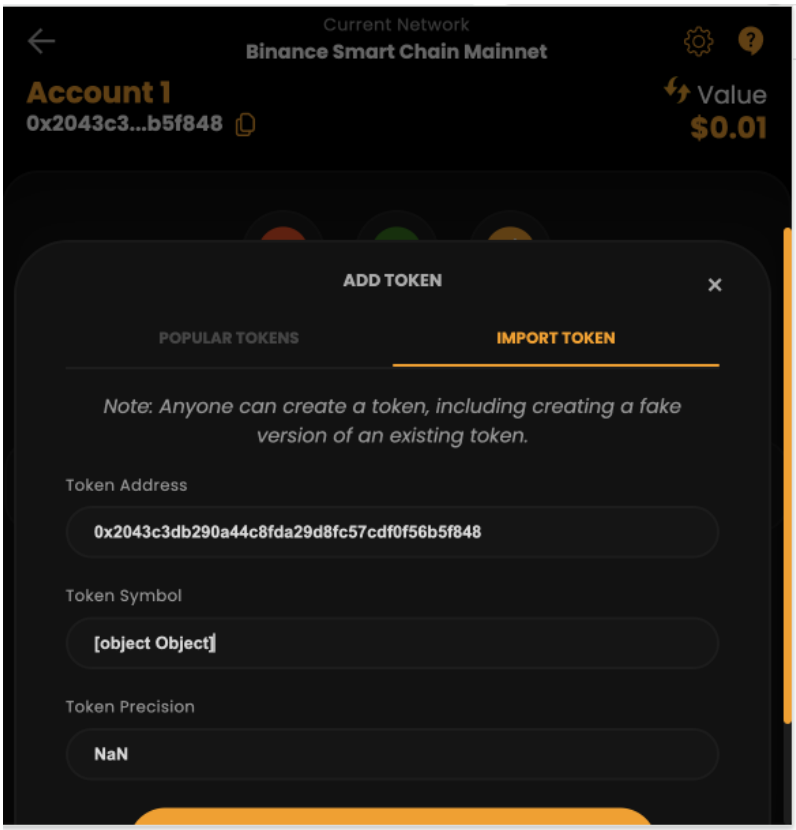
The wallet features a functionality that allows users to import new tokens. A issue exists where importing an invalid token results in a crash of certain features within the application, thus compromising its stability.

Impact

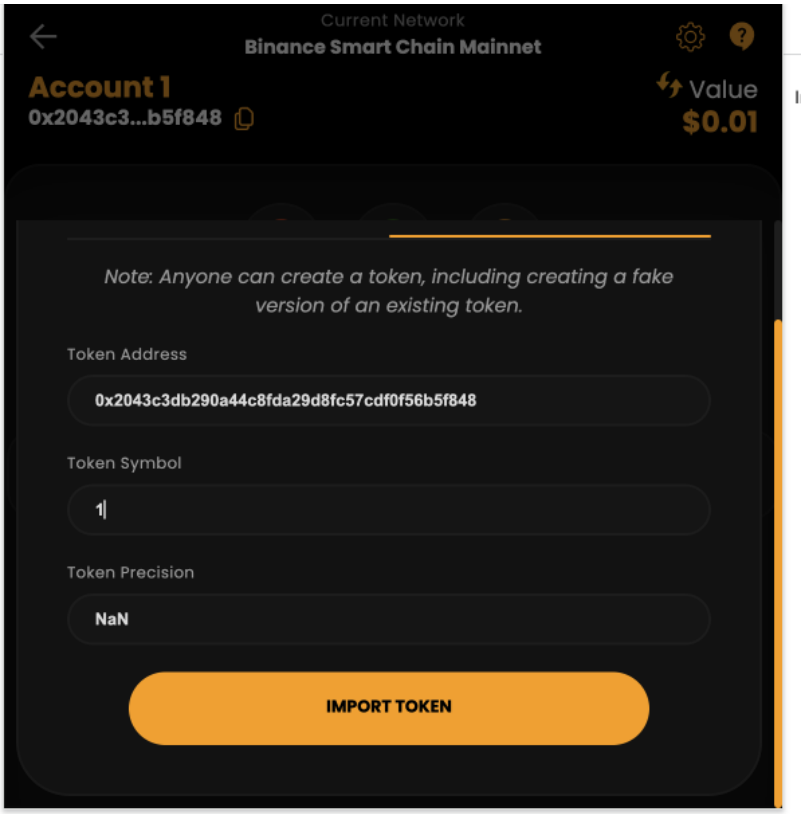
Key functionalities of the wallet are rendered unusable after the crash, imposing on users the inconvenient workaround of having to reinstall the wallet to restore these features.

Proof of Concept

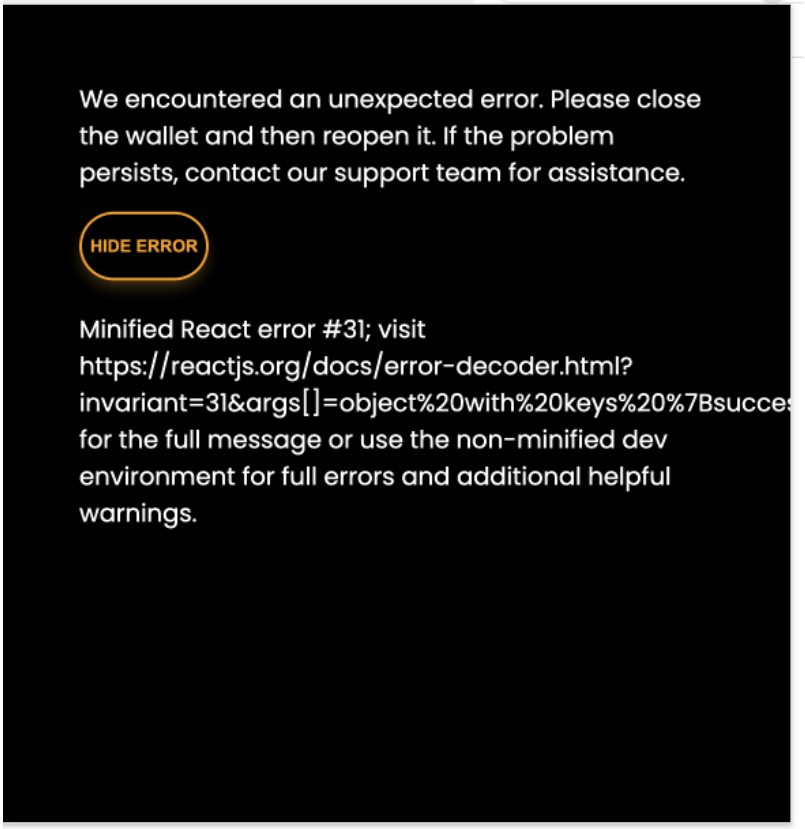
1. Import an address that is not a token, such as "0x2043c3db290a44c8fda29d8fc57cdf0f56b5f848"



2. Modify the token name to 1 and click "IMPORT Token"



3. The wallet will then enter the error page, and the token import/remove page becomes unusable, even after relaunching the wallet.



Recommendation

It is recommended that the wallet application implement robust input validation and error handling mechanisms to gracefully manage the import of invalid tokens, ensuring that such an action does not cause features within the wallet to crash.

Alleviation

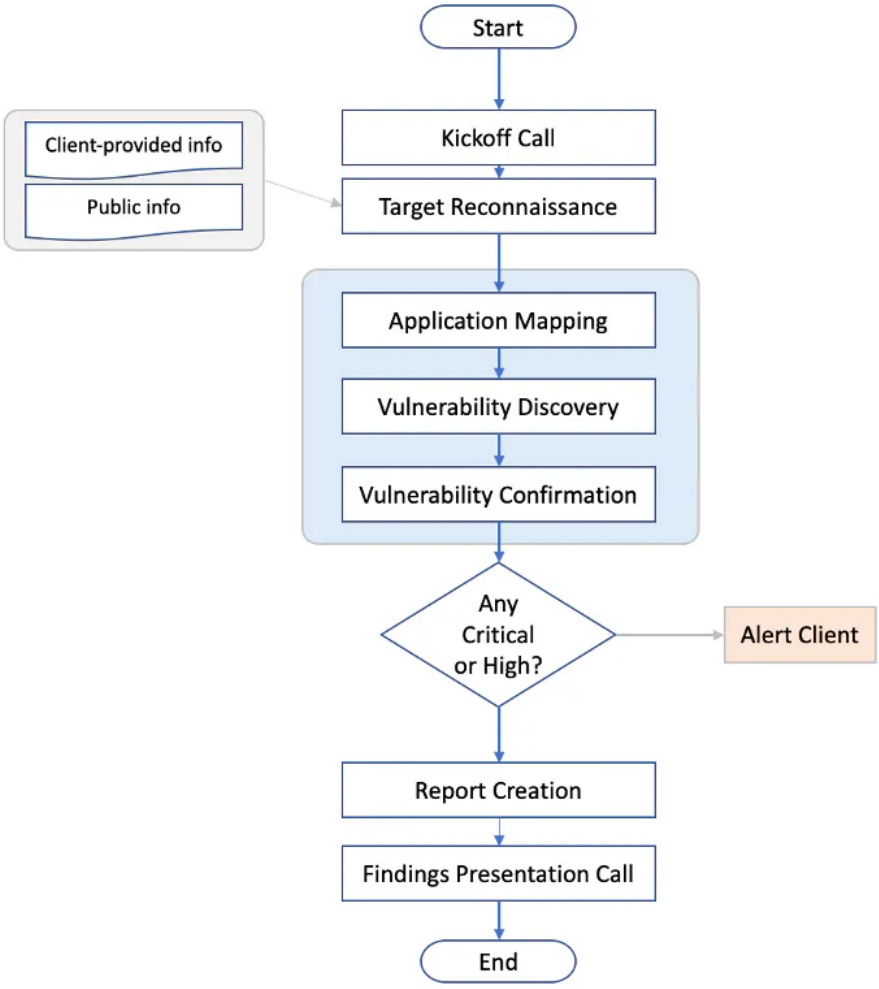
Fixed in commit 7094b5b2deecf64fd0333a8f3af46648d9b2f7f1.

APPENDIX | INTERNET MONEY WALLET

Methodology

CertiK uses a comprehensive penetration testing methodology which adheres to industry best practices and standards in security assessments including from OWASP (Open Web Application Security Project), NIST, PTES (Penetration Testing Execution Standard).

Below is a flowchart of our assessment process:



DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

CertiK | Securing the Web3 World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.