CONTRACT WOLF

Security Assessment

MetChain Wallet

Verified on 11/08/2023

SUMMARY

Project	CHAIN	METHODOLOGY
MetChain Wallet	MetChain	Manual & Automatic Analysis

FILES	DELIVERY	TYPE
Single	11/08/2023	Standard Audit

0	0	0	0	0	0
Total Findings	Critical	Major	Medium	Minor	Informational

🟥 0 Critical	An exposure that can affect the contract functions in several events that can risk and disrupt the contract
🟧 0 Major	An exposure that can affect the outcome when using the contract that can serve as an opening in manipulating the contract in an unwanted manner
🟧 0 Medium	An opening that could affect the outcome in executing the contract in a specific situation
⬜ 0 Minor	An opening but doesn't have an impact on the functionality of the contract
🟦 0 Informational	An opening that consists information but will not risk or affect the contract

STATUS ✔️ **AUDIT PASSED**

TABLE OF CONTENTS | MetChain Wallet

DISCLAIMER | MetChain Wallet

ContractWolf audits and reports should not be considered as a form of project's "Advertisement" and does not cover any interaction and assessment from "Project Contract" to "External Contracts" such as PancakeSwap, UniSwap, SushiSwap or similar.

ContractWolf does not provide any warranty on its released report and should not be used as a decision to invest into audited projects.

ContractWolf provides a transparent report to all its "Clients" and to its "Clients Participants" and will not claim any guarantee of bug-free code within its **SMART CONTRACT**.

ContractWolf's presence is to analyze, audit and assess the Client's Smart Contract to find any underlying risk and to eliminate any logic and flow errors within its code.

Each company or project should be liable to its security flaws and functionalities.

SCOPE OF WORK | MetChain Wallet

MetChain Wallet team has agreed and provided us with the files that need to be tested (*Github, BSCscan, Etherscan, Local files etc*). The scope of audit is the main contract.

The goal of this engagement is to identify if there is a possibility of security flaws in the implementation of smart contract and its systems.

ContractWolf will be focusing on contract issues and functionalities along with the project claims from smart contract to their website, whitepaper, repository which has been provided by **MetChain Wallet**.

AUDITING APPROACH | MetChain Wallet

Every line of code along with its functionalities will undergo manual review to check for security issues, quality of logic and contract scope of inheritance. The manual review will be done by our team that will document any issues that they discovered.

METHODOLOGY

The auditing process follows a routine series of steps :

1. Code review that includes the following :
   - Review of the specifications, sources and instructions provided to ContractWolf to make sure we understand the size, scope and functionality of the smart contract.
   - Manual review of code. Our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities, underlying and hidden security flaws.

2. Testing and automated analysis that includes :
   - Testing the smart contract function with common test cases and scenarios to ensure that it returns the expected results.

3. Best practices and ethical review. The team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security and control within the smart contract.

4. Recommendations to help the project take steps to eliminate or minimize threats and secure the smart contract.

TOKEN DETAILS | MetChain Wallet

MetChain aims to provide the next generation metaverse and gaming ecosystem built on Metchains three layered blockchain.

SOURCE

Source	*https://github.com/Metchain/MetblockD/tree/main/newwallet*

SECURITY AUDIT | MetChain Wallet

Auditing the Security of MetChain Wallet

Project Introduction

Metchain is a bitcoin-like wallet that utilizes a BIP32 & Base58 encoding model for wallet addresses and ECDSA encryption for enhanced security. This audit aims to assess the overall security posture of the MetChain wallet, identifying potential vulnerabilities and recommending mitigation strategies.

Security Analysis

Seed Storage

MetChain commendably avoids storing seeds in databases, eliminating the risk of unauthorized access or data breaches. The seeds are encrypted and stored locally on the user's device, providing an additional layer of protection.

Seed Duplication Prevention

Metchain's incorporation of a unix timestamp in the seed generation process effectively prevents seed duplication. This ensures that each user possesses a unique seed, reducing the likelihood of compromised seeds being used to access multiple accounts.

HTTPS Encryption

Metchain's implementation of HTTPS encryption for communication with its node servers safeguards user data from interception and tampering during transmission. This ensures that sensitive information remains confidential and protected from unauthorized access.

Hot Wallet Classification

Metchain's reliance on online node servers classifies it as a "hot wallet," implying an inherent risk associated with online connectivity. However, the wallet's utilization of encryption and secure communication protocols mitigates this risk to a considerable extent.

Vulnerability Assessment

Despite its robust security measures, MetChain is not entirely immune to potential vulnerabilities. One area of concern is the potential for malware infections on the user's device. If a malicious program gains access to the device, it could potentially intercept and decrypt the encrypted seeds, compromising the user's wallet.

Recommendations for Enhanced Security

Multi-Signature Support

Implementing multi-signature functionality would further enhance the security of Metchain's future transactions. This would require multiple signatures from authorized parties before a transaction can be executed, adding an extra layer of protection against unauthorized access or fraudulent transactions.

Hardware Wallet Integration

Providing integration with hardware wallets would offer users an even more secure storage option for their seeds. Hardware wallets are physical devices specifically designed to safeguard sensitive cryptographic keys, providing an additional barrier against malware attacks.

Regular Security Audits

Conducting regular security audits is crucial for identifying and addressing emerging vulnerabilities. These audits should be performed by independent security experts to ensure objectivity and thoroughness.

Conclusion

MetChain wallet exhibits a strong commitment to security, employing various measures to protect user funds and data. The wallet's implementation of encrypted seeds, seed duplication prevention, HTTPS encryption, and secure communication protocols significantly mitigates potential security risks. However, the potential for malware infections and the inherent risks associated with **hot wallets** warrant further consideration and the implementation of additional security measures, such as multi-signature support, hardware wallet integration, and regular security audits. By continuously enhancing its security posture, Metchain can maintain its position as a trusted and secure on-chain wallet.

AUDIT COMMENTS | MetChain Wallet

This audit covers the commit ID/Hash information below, Future changes of folder "metwallet" will not be covered by this audit until verified for an update.

commit hash : 2fc613d1ef3e6b935888e9d2ae167d03101e52cc

or

https://github.com/Metchain/MetblockD/commit/2fc613d1ef3e6b935888e9d2ae167d03101e52cc

CONTRACTWOLF

Blockchain Security - Smart Contract Audits