CONTRACT WOLF

Security Assessment

MetChain Wallet

Verified on 06/20/2023

SUMMARY

Project	CHAIN	METHODOLOGY
MetChain Wallet	Ethereum	Manual & Automatic Analysis

FILES	DELIVERY	TYPE
Single	06/20/2023	Standard DAPP Audit

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

🟥 0 Critical	0 Pending		An exposure that can affect the contract functions in several events that can risk and disrupt the contract
🟧 0 Major	0 Pending		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	0 Pending		An opening that could affect the outcome in executing the contract in a specific situation
⬜ 0 Minor	0 Pending		An opening but doesn't have an impact on the functionality of the contract
🟦 0 Informational	0 Pending		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**.
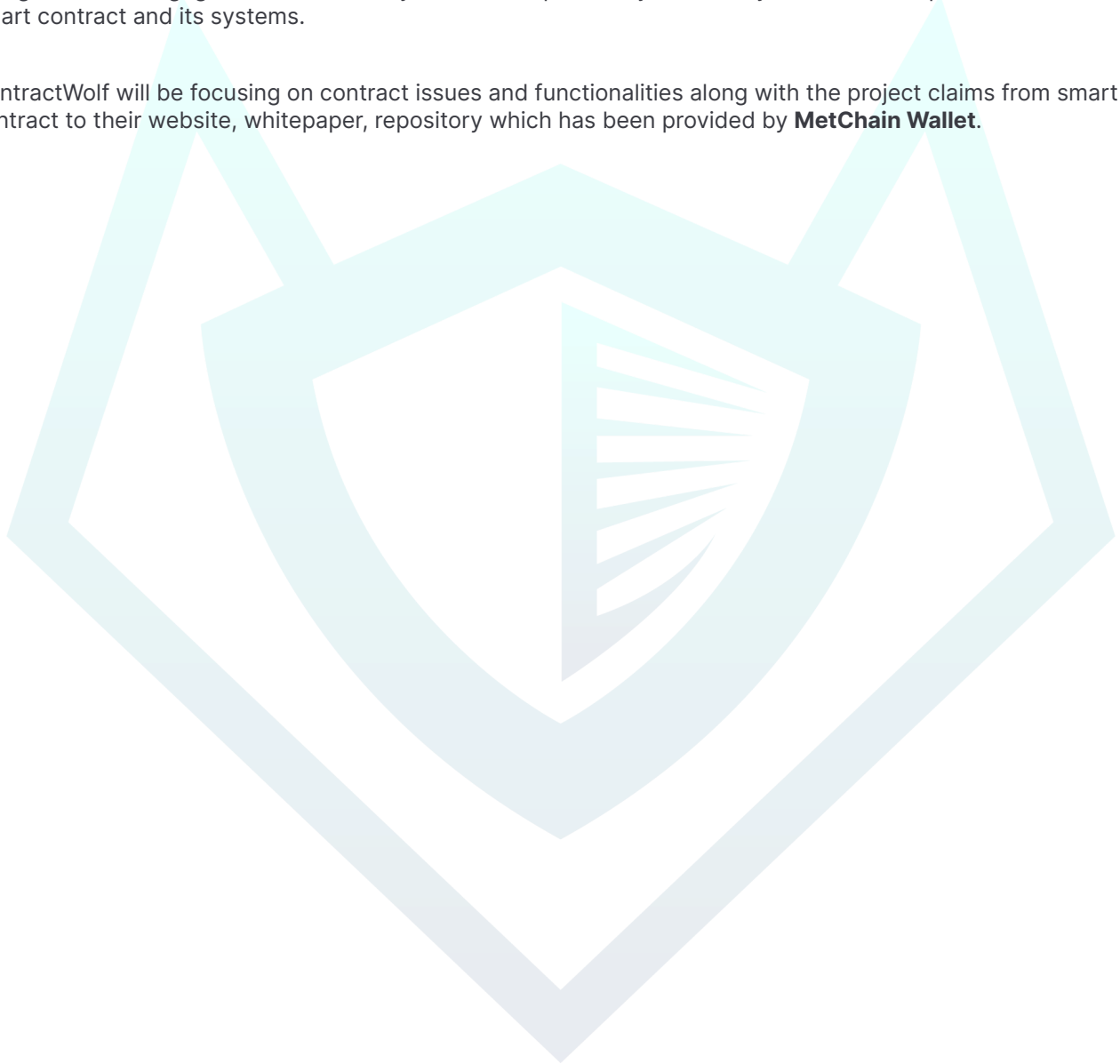
AUDITING APPROACH | MetChain Wallet

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

MetchainWallet is an open source implementation of the backend of https://wallet.metchain.tech. The frontend, which includes HTML, CSS & JavaScript was adapted from (and originally developed by) https://metchain.tech .

SOURCE

Source   *https://github.com/blockchainspectre/WebWallet*

FINDINGS | MetChain Wallet

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

This report has been prepared to state the issues and vulnerabilities for MetChain Wallet through this audit. The goal of this report findings is to identify specifically and fix any underlying issues and errors

ID	Title	File & Line #	Severity	Status
–	–	–	N/A	• N/A

CW ASSESSMENT | MetChain Wallet

ContractWolf Vulnerability and Security Tests

Faces associated with your website
Completed - No findings

Leaked Accounts Check
Completed - No findings

Sensitive Public Information Check
Completed - No findings

Subdomains found
Completed - Discovered **11** findings

- explore.metchain.tech
- *.metchain.tech
- metchain.tech
- nft.metchain.tech
- rpc.metchain.tech
- rpc.test.metchain.tech
- swap.metchain.tech
- test.metchain.tech
- testmine.metchain.tech
- wallet.metchain.tech

Server software and technologies found
Completed - Discovered **8** findings

Google Font API	jsDelivr	particles.js	Ubuntu	jQuery UI	Apache 2.4.52	Chart.js
Font scripts	CDN	JavaScript graphics	Operating systems	JavaScript libraries	Web servers	JavaScript graphics

jQuery
JavaScript libraries

Risk
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation
We recommend all server and technologies are relevant to the application and up to date.

Missing HTTP headers found
Completed - Discovered **11** findings

Rule	Message
Cache-Control	Value does not match security policy
Content-Security-Policy	Header not included in response
Pragma	Header not included in response
Referrer-Policy	Header not included in response
Server	Header should not be returned
Set-Cookie - XSRF-TOKEN	Must-Contain directive missed
Set-Cookie - metchainwebwallet_session	Must-Contain directive missed
Strict-Transport-Security	Header not included in response
X-Content-Type-Options	Header not included in response
X-Frame-Options	Header not included in response

No Issues | DAPP Audited

The purpose of this DAPP audit is to make sure that Metchain team complies with safety & security measurement since the DAPP will be used by public users.

This DAPP has been audited with the commit hash id of : `ac18b11`

ContractWolf did not find any major issues and marked this DAPP <u>safe</u> to be interacted with.

AUDIT COMMENTS | MetChain Wallet

DAPP audit comment for a non-technical perspective

- No backdoors found
- Safe to use/interact (Connect Wallet)
- Saving data through email
- This DAPP(wallet) is only exclusive for Metchain's ecosystem
- This DAPP has a centralized application

CONTRACTWOLF

Blockchain Security - Smart Contract Audits