Penetration Testing Report

Document Properties

Title	White Box Penetration Testing Report
Version	V 1.0
Author	Thinking
Pen-testers	Cos, Blue, Thinking
Reviewed By	Blue
Classification	Public

Version control

Version	Date	Author	Description
V 1.0	06.23, 2021	Thinking	Final Draft

Table of Contents

1.Basic information

The SlowMist security team conducted the penetration testing on the Rabby chrome extension project under the authorization of Rabby team. This report is written based on the test process and results, to help Rabby team understand the safety of the target business system, and guide Rabby team to fix and rectify it.

1.1 Scope of work

This security assessment covers the penetration testing of Rabby chrome extension The assessment was carried out from a white box perspective, with the only supplied information being the tested chrome extension. No other information was assumed at the start of the assessment.

Audited Version:

https://github.com/RabbyHub/Rabby/tree/579f4fc7386d9af0327dbe9be8eb278211425c9d

Fixed Version:

https://github.com/RabbyHub/Rabby/tree/c98a16398173f391a66fbe032c96515ba678dd8f

1.2 Testers and Timeline

This penetration testing is carried out within the timeline agreed in advance as follows:

Timeline			
Start Date/Time	06.07,2021	**End Date/Time**	06.18,2021

The participants of this penetration testing are shown as follows:

List of Testers			
Organization	**Role**	**Name**	**Contact**
SlowMist Security Team	The Company Founder	Cos	cos@slowmist.com
SlowMist Security Team	CTO	Blue	blue@slowmist.com
SlowMist Security Team	Leader of Business Security Management	Thinking	thinking@slowmist.com

1.3 Test content

The content of this test is the chrome-extension wallet security test of SlowMist, which is carried out in accordance with the OWASP security test guide, with reference to the CVSS vulnerability rating standard. The SlowMist security team adopts the strategy of "mainly white box, supplemented by black and grey box" to conduct a complete security test of the project in the way that is closest to the real attack.

1.4 Other explanatory information

Application security test method of SlowMist:

Black box testing	Conduct security tests externally from the attacker's perspective.

Grey box testing	Through communication with the person in charge of the project, investigate the internal security construction of the project, conduct the security assessment and the security test according to the investigation results, observe the internal operation status, and mining weaknesses.
White box testing	Based on open source and non-open source code, mining vulnerability(ies) in nodes, SDK, sites and other programs.

Application security risk level of SlowMist standard:

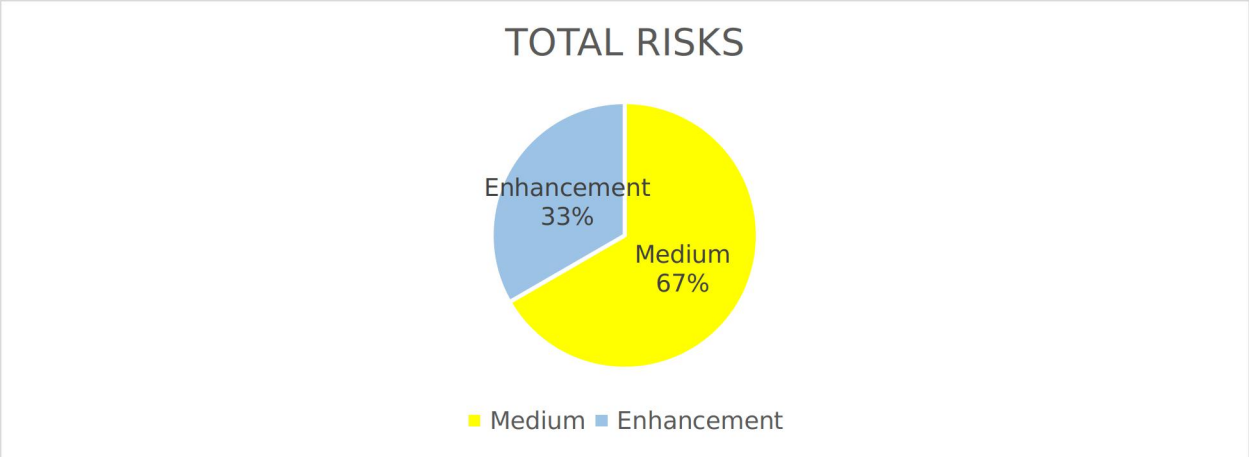
Critical	The critical vulnerability can have a significant impact on the security of business systems or user information, and it is strongly recommended to fix the critical vulnerability(ies).
High	The high-risk vulnerability will affect the normal operation of the business system. It is strongly recommended to fix the high-risk vulnerability.
Medium	Medium vulnerability will affect the operation of the business system. It is suggested to fix the medium vulnerability.
Low	Low-risk vulnerabilities may affect the operation of the business system in certain scenarios. It is recommended that the project party evaluate and consider whether these issues need to be fixed.
Weakness	Theoretically there are security risks, but it is very difficult to reproduce in engineering, the system will be more robust after adding security policy.
Enhancement suggestion	There will be no problems at present, but as the system develops, it may become a vulnerability in the future.

2.Test summary

2.1 Summary of Findings

Level	Number of Risks
Critical	0
High	0
Medium	2
Low	0
Weakness	0
Enhancement suggestion	1

2.2 Total Risks



3.Test Results

3.1 Transaction Process Security Test

NO.	Check	Response	Threat	OK
1	Does the signature have a clear reminder?	● DApp's signature request will be reminded. ● Reminder contains the domain. ● The request needs confirmation.	Passed	√
2	Where is the implementation location of the signature?	● The transaction signature operation is performed in "backgroundscript".	Passed	√
3	Is there an issue about the transfer prompt?	● No "false top-up" vulnerabilities found.	Passed	√
4	How to configure the broadcast node?	● When the broadcast RPC interface is initialized, the configuration of Node is read by "backgroundscript". ● Broadcast RPC can be set through the popup. ● DApp cannot modify the RPC interface of transaction broadcast.	Passed	√

3.2 Private Key/Mnemonic Phrase Security Test

NO.	Check	Response	Threat	OK
1	How is the Private key/Mnemonic Phrase generated ?	● Use bip39.generateMnemonic(128) to generate mnemonic words. ● Generated in the "backgroundscript".	Passed	√
2	How is the Private key/Mnemonic Phrase stored ?	● Use aes-256-ctr to encrypt storage. ● Using KDF for protection. ● Stored in chrome local folder ● Using random IV.	Passed	√
3	How is the Private key/Mnemonic Phrase used ?	● When using the private key and mnemonic words, it is required to unlock the wallet, and there is a sign prompt. ● Password verification for export Private key/Mnemonic Phrase can be bypassed.	Medium	**Fixed**

4	How to get random seeds ?	● The random seeds are obtained by using crypto.getRandomValues, that is the best security practice.	Passed	√
5	What encryption method is used ?	● The aes-256-ctr encryption method encrypts the password using KDF for protection.	Passed	√

3.3 Web Front End Security Test

NO.	Check	Response	Threat	OK
1	Is there any XSS issue found ?	● No security issues found.	Passed	√
2	What is the result of checking the third-party JS ?	● The version of css-what and dns-packet is too low.	Enhancement	√

3.4 Communications Security Test

NO.	Check	Response	Threat	OK
1	Does RPC use encryption for communication ?	● Use HTTPS for encrypted communication.	Passed	√
2	How does the extension communicate with the DApp ?	● the extension uses window.addEventListener to communicate with the DApp.	Passed	√
3	How does the extension communicate with itself internal wallet?	● the extension uses runtime.connect to communicate with the itself.	Passed	√

3.5 Business Logic Test

NO.	Check	Response	Threat	OK
1	Is there an access control check for export Private key/Mnemonic Phrase?	● Only after unlocking the wallet can Private key/Mnemonic Phrase be exported.	Passed	√
2	Does the wallet object set null after the wallet is locked ?	● After the wallet is locked, the password can not be obtained.	Passed	√
3	Is the business logic performed as expected ?	● The window.addEventListener judge the origin of the message, and any site can initiate a signature request need authorization to connect to the wallet. ● Add watch address can be any string. ● Lack of mnemonic verification mechanism.	Medium	**Fixed**

Disclaimer

Xiamen SlowMist Technology Co., Ltd.(hereinafter referred to as "SlowMist") issues this report only based on the facts that have happened or existed before the report is issued, and will take the corresponding responsibilities for the report based on these facts. Regarding any unknown vulnerabilities or security incidents that happen or exist after the issue of this report, SlowMist cannot verify their security conditions and will not be responsible for them. All of the security audits analysis and other contents consisted in this report are only based on the files and documents provided to SlowMist by information providers(hereinafter referred to as "provided documents"). SlowMist assumes that the provided documents are not under any of these circumstances, such as being absent, being tampered, being abridged or being concealed. If the information of the provided documents were absent, tampered, abridged, concealed, or did not conform to the reality, SlowMist would not be responsible for any of the loss or disadvantages caused by these circumstances. SlowMist only performs the appointed security audits for the security condition of this project and issues this report. SlowMist is not responsible for the background of this project or any other circumstances.

Reference

[1]”Common Vulnerability Scoring System version 3.1”：https://www.first.org/cvss/specification-document

[2] “国家区块链漏洞库《区块链漏洞定级细则》”: https://bc.cnvd.org.cn/notice_info?num=51d78f7d7334ce3d1f7bf62b4471772d

[3] “Security Analysis of Chrome Extensions”: https://arxiv.org/pdf/1403.3235.pdf

[4]”OWASPLondon_PostMessage_Security_in_Chrome_Extensions”: https://owasp.org/www-chapter-london/assets/slides/OWASPLondon_PostMessage_Security_in_Chrome_Extensions.pdf

[5]”Hunting postMessage Vulnerabilities”: https://docs.ioin.in/writeup/www.exploit-db.com/_docs_40287_pdf/index.pdf

[6]”Web3 Secret Storage Definition”:https://github.com/ethereum/wiki/wiki/Web3-Secret-Storage-Definition

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist