Penetration Testing Report

Document Properties

Title	Black Box Penetration Testing Report
Version	V 1.0
Author	xu
Pen-testers	Xu, kong, yudan, thinking, reborn
Reviewed By	blue
Classification	Public

Version control

Version	Date	Author	Description
V 1.0	05.22,2021	xu	Final Draft
V 1.1	09.24, 2021	reborn	Fix Review

Table of Contents

1.Basic information

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

1.1 Scope of work

This security assessment covers the penetration testing of TronLink iOS App,The assessment was carried out from a black box perspective, with the only supplied information being the tested iOS App. No other information was assumed at the start of the assessment.

Download link：

https://tronlink.org

Version： v4.0.1

MD5: dbec124e88b4460a60ac6c3b2f101552

1.2 Tester and Timeline

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

Timeline			
Start Date/Time	04.21,2021	**End Date/Time**	10.24,2021

The participants of this penetration testing are shown as follows:

List of Testers			
Organization	**Role**	**Name**	**Contact**
SlowMist Security Team	Security Engineer	xu	mx@slowmist.com
SlowMist Security Team	Security Engineer	kong	kong@slowmist.com
SlowMist Security Team	Security Engineer	yudan	yudan@slowmist.com
SlowMist Security Team	Security Engineer	reborn	wyl@slowmist.com
SlowMist Security Team	CTO	blue	blue@slowmist.com
SlowMist Security Team	Leader of SlowMist Security Team	Thinking	thinking@slowmist.com

1.3 Test content

The content of this test is the TronLink iOS App 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 black box, supplemented by 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:

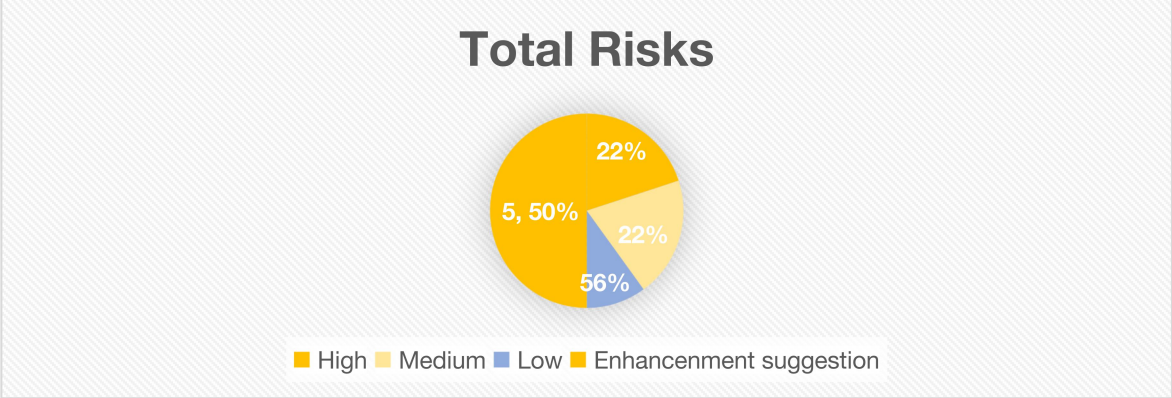
Critical	The critical vulnerability can have a significant impact on the security of business systems or user information, and it is strongly recommended to fix the critical vulnerability(ies).
High	The high-risk vulnerability will affect the normal operation of the business system. It is strongly recommended 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	Fixed
Critical	0	0
High	2	2
Medium	1	1
Low	1	1
Weakness	0	0
Enhancement suggestion	5	5

2.2 Total Risks



2.3 Summary conclusion

The SlowMist security team used manual and analytical tools to audit the TronLink project. During the audit, we found 2 high risks, 1 medium risks, 1 low risks and 5 suggestions. And 2 high risks, 1 medium risks, 1 low risk and 5 suggestions were confirmed and fixed, There are no other issues found.

3.Test Results

3.1 General Security Test

NO.	Check	Response	Threat	OK
1	Does application attempt to detect jailbreak?	● Jailbreak trace checks are performed at every application initialization. ● If jailbreak is detected a warning message is displayed.	Passed	√
2	Are there any SSL pinning for TLS connections ?	● No SSL pinning implemented.	Enhancement suggestion	Fixed
3	Is video and screenshot check?	● There are obvious risk warnings.	Passed	√
4	Is there a clipboard check?	● There is an obvious risk warning broadcast. ● The private key resides in memory for a long time.	Enhancement suggestion	Fixed
5	Is there obfuscation when the app hangs?	● There is no obfuscation when the app is suspended or when switching between apps.	Medium	Fixed

3.2 Private Key/Mnemonic Phrase Security Test

NO.	Check	Response	Threat	OK
1	How can user fetch private keys?	• Can only be done by using “export keys” feature via application user interface	Passed	√
2	How is the Private key/Mnemonic Phrase stored?	• Use md5 to encrypt user password. • Stored in SQLite without using PBKDF for protection. • Stored in json file with using KDF for protection.	High	Fixed
3	Can user restore or backup private keys with iTunes or other application backups?	• File that keeps key data is included from iTunes and other application backups.	High	Fixed
4	How exported keys are protected?	• Exported keys are encrypted with user provided password. • The aes-128-ctr encryption method encrypts the password with using KDF for protection.	Passed	√

3.3 Risk Control Security Test

NO.	Check	Response	Threat	OK
1	Is there a malicious address check?	• No check for malicious addresses.	Enhancement suggestion	Fixed
2	Is there an anti-phishing check?	• No phishing detection when accessing third-party DApp.	Enhancement suggestion	Fixed
3	Is there a “fake token” check?	• No obvious “fake token” prompt.	Enhancement suggestion	Fixed

3.4 Other Security Test

NO.	Check	Response	Threat	OK
1	Is there a DApp interactive security reminder ?	• The wallet address can be obtained directly through window.tronWeb.defaultAddress/address without operation confirmation. • Signature and transaction operations are initiated by calling tronWeb.trx.sendRawTransaction and are not performed in the wallet itself.	Low	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]”Mobile App Security Requirements and Verification”: https://github.com/OWASP/owasp-masvs/releases/download/v1.3/OWASP_MASVS-1.3-en.pdf

[4]”Mobile Security Testing Guide (MSTG)”:https://mobile-security.gitbook.io/mobile-security-testing-guide/

[5]”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