Tesa Extension

EXTENSION AUDIT REPORT

November 2024

ExVul

www.exvul.com

Table of Contents

1. EXECUTIVE SUMMARY

Exvul Web3 Security was engaged by Tesa to review Extension implementation. The assessment was conducted in accordance with our systematic approach to evaluate potential security issues based upon customer requirement. The report provides detailed recommendations to resolve the issue and provide additional suggestions or recommendations for improvement.

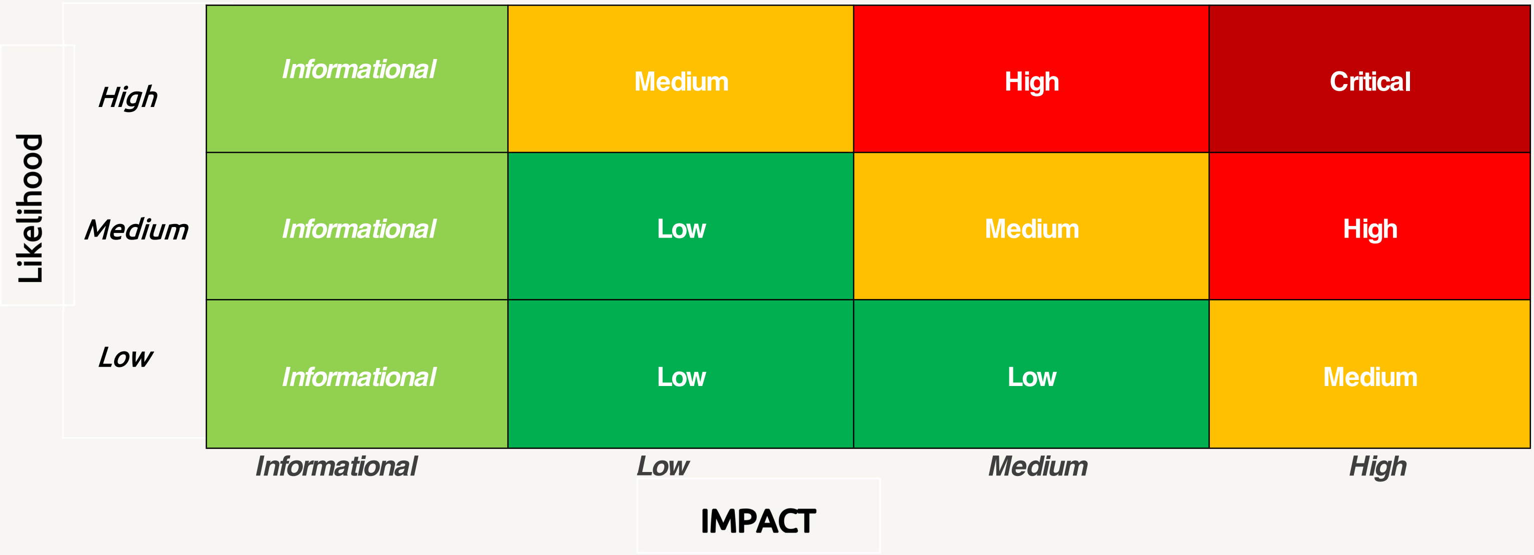
The outcome of the assessment outlined in chapter 3 provides the system's owners a full description of the vulnerabilities identified, the associated risk rating for each vulnerability, and detailed recommendations that will resolve the underlying technical issue.

1.1 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [10] which is the gold standard in risk assessment using the following risk models:

- Likelihood: represents how likely a particular vulnerability is to be uncovered and exploited in the wild.
- Impact: measures the technical loss and business damage of a successful attack.
- Severity: determine the overall criticality of the risk.

Likelihood can be: High, Medium and Low and impact are categorized into for: High, Medium, Low, Informational. Severity is determined by likelihood and impact and can be classified into five categories accordingly, Critical, High, Medium, Low, Informational shown in table 1.1.



Likelihood				
High	Informational	Medium	High	Critical
Medium	Informational	Low	Medium	High
Low	Informational	Low	Low	Medium
	Informational	Low	Medium	High
	IMPACT			

Table 1.1 Overall Risk Severity

To evaluate the risk, we will be going through a list of items, and each would be labelled with a severity category. The audit was performed with a systematic approach guided by a comprehensive assessment list carefully designed to identify known and impactful security issues. If our tool or analysis does not identify any issue, the contract can be considered safe regarding the assessed item. For any discovered issue, we might further deploy contracts on our private test environment and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.2.

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.

- Code and business security testing: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

Category	Assessment Item
Basic Coding Assessment	Apply Verification Control
	Authorization Access Control
	Forged Transfer Vulnerability
	Forged Transfer Notification
	Numeric Overflow
	Transaction Rollback Attack
	Transaction Block Stuffing Attack
	Soft Fail Attack
	Hard Fail Attack
	Abnormal Memo
	Abnormal Resource Consumption
	Secure Random Number
Advanced Source Code Scrutiny	Asset Security
	Cryptography Security
	Business Logic Review
	Source Code Functional Verification
	Account Authorization Control
	Sensitive Information Disclosure
	Circuit Breaker
	Blacklist Control
	System API Call Analysis
	Contract Deployment Consistency Check
Additional Recommendations	Semantic Consistency Checks
	Following Other Best Practices

Table 1.2: The Full List of Assessment Items

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [14], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development.

2. FINDINGS OVERVIEW

2.1 Project Info And Contract Address

Project Name: Tesa

Audit Time: November 7nd, 2024 – November 13th, 2024

File Name	HASH
Tesa	https://tesa.top/extension

2.2 Summary

Severity	Found	
Critical	0	
High	0	
Medium	0	
Low	2	🟦🟦
Informational	0	

2.3 Key Findings

ID	Severity	Findings Title	Status	Confirm
NVE- 001	Low	Jwt Token is recommended to be stored in sessionStorage	Ignore	Confirmed
NVE- 002	Low	The time interval between price updates may be too long	Ignore	Confirmed

Table 2.3: Key Audit Findings

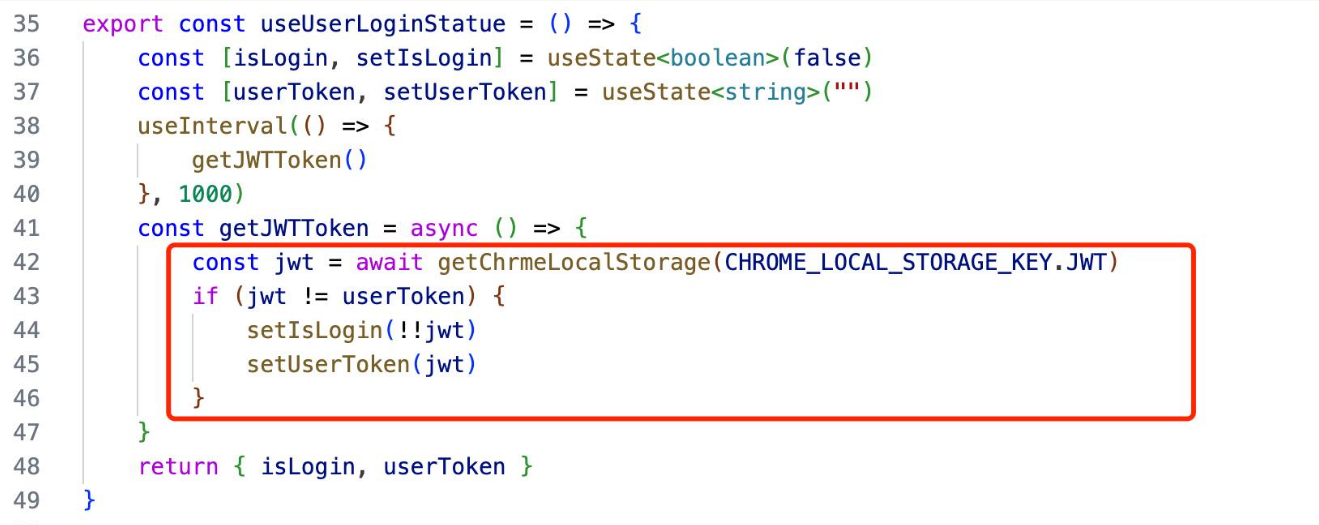
3. DETAILED DESCRIPTION OF FINDINGS

3.1 Jwt Token is recommended to be stored in sessionStorage

ID:	NVE-001	Location:	src/hooks/index.ts
Severity:	Low	Category:	Business Issues
Likelihood:	Low	Impact:	Low

Description:

The getJwtToken function is used in useUserLoginStatus to obtain the JWT token, which is currently stored in chrome.storage. It is recommended to store the JWT token in sessionStorage instead of chrome.storage.



```
export const useUserLoginStatue = () => {
    const [isLogin, setIsLogin] = useState<boolean>(false)
    const [userToken, setUserToken] = useState<string>("")
    useInterval(() => {
        getJWTToken()
    }, 1000)
    const getJWTToken = async () => {
        const jwt = await getChrmeLocalStorage(CHROME_LOCAL_STORAGE_KEY.JWT)
        if (jwt != userToken) {
            setIsLogin(!!jwt)
            setUserToken(jwt)
        }
    }
    return { isLogin, userToken }
}
```

Recommendations:

It is recommended to store the JWT token in sessionStorage instead of chrome.storage.

Result: Confirmed

Fix Result: Ignore

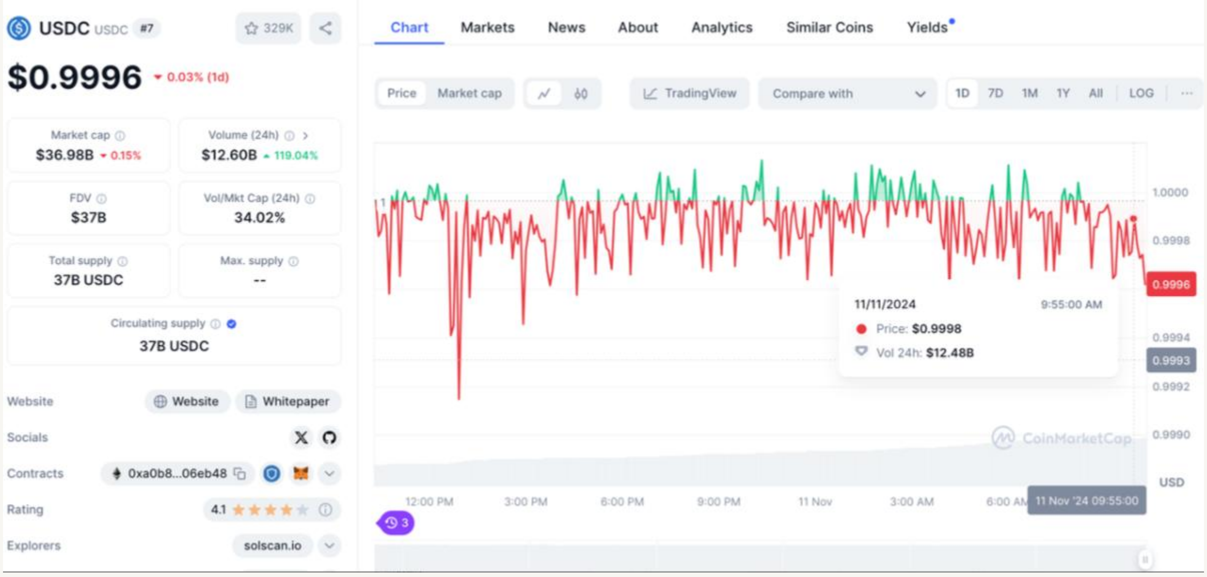
The client replied that our jwt has no expiration date, so it needs to be placed in localstorage.

3.2 The time interval between price updates may be too long

ID:	NVE-002	**Location:**	src/hooks/index.ts
Severity:	Low	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Low

Description:

The current price update time is every 60 seconds. The price of USDC fluctuates within a certain range and is not very stable. If there are large changes in a short period of time, the price may not be updated in time.



USDC USDC #7

$0.9996 ▾ 0.03% (1d)

Market cap $36.98B ▾ 0.15%

Volume (24h) $12.60B ▴ 119.04%

FDV $37B

Vol/Mkt Cap (24h) 34.02%

Total supply 37B USDC

Max. supply --

Circulating supply 37B USDC

Website: Website, Whitepaper

Contracts: 0xa0b8...06eb48

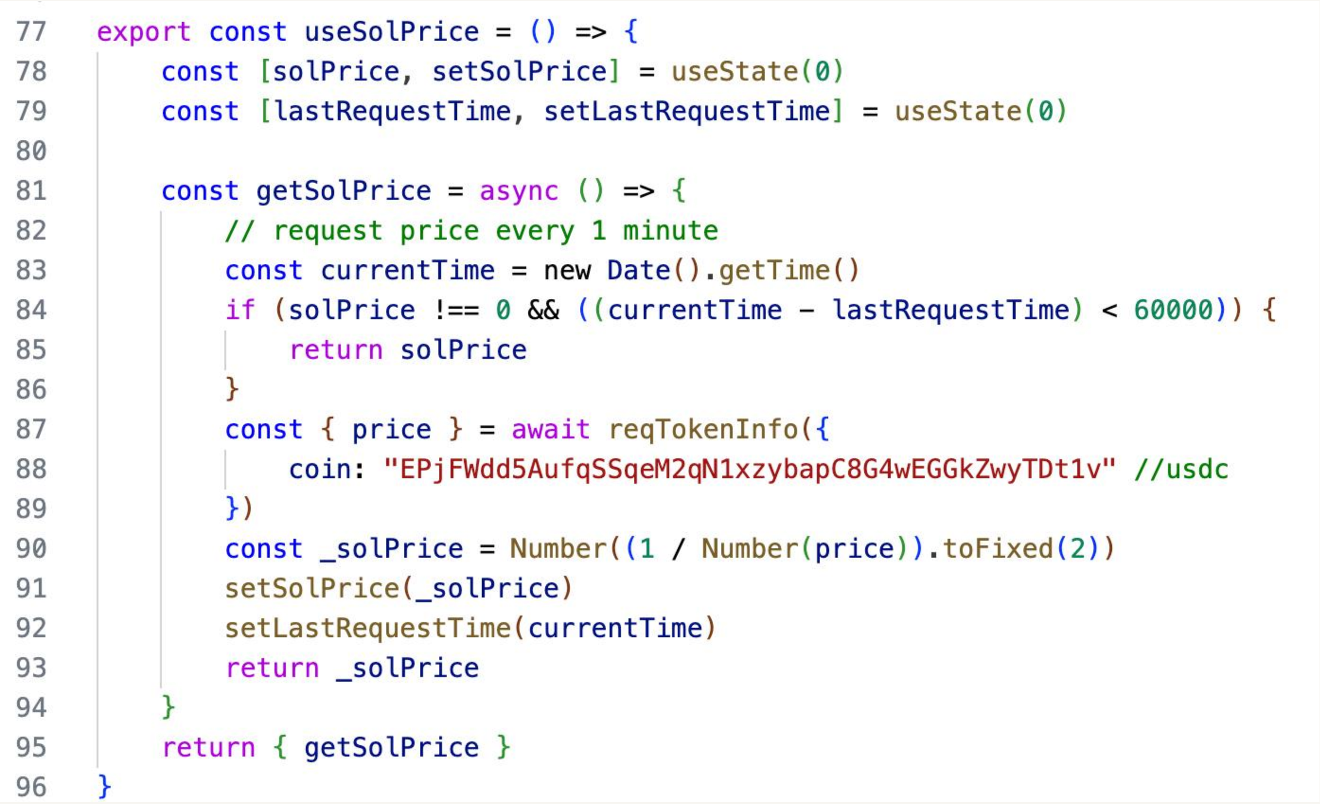
Rating: 4.1

Explorers: solscan.io

11/11/2024 9:55:00 AM

Price: $0.9998

Vol 24h: $12.48B



```
export const useSolPrice = () => {
    const [solPrice, setSolPrice] = useState(0)
    const [lastRequestTime, setLastRequestTime] = useState(0)

    const getSolPrice = async () => {
        // request price every 1 minute
        const currentTime = new Date().getTime()
        if (solPrice !== 0 && ((currentTime - lastRequestTime) < 60000)) {
            return solPrice
        }
        const { price } = await reqTokenInfo({
            coin: "EPjFWdd5AufqSSqeM2qN1xzybapC8G4wEGGkZwyTDt1v" //usdc
        })
        const _solPrice = Number((1 / Number(price)).toFixed(2))
        setSolPrice(_solPrice)
        setLastRequestTime(currentTime)
        return _solPrice
    }
    return { getSolPrice }
}
```

Recommendations:

Reduce the update interval. Consider shortening the update interval, such as adjusting it to 10 seconds or 15 seconds, so that prices can be updated more frequently during fluctuations. Dynamic update interval. Dynamically adjust the update frequency according to market fluctuations. For example, when a price fluctuation of more than a certain percentage (such as 0.5% or 1%) is detected, the update interval is temporarily shortened to update the price more timely.

Result: Confirmed

Fix Result: Ignore

The customer replied that our front-end token response time is matched with the background price refresh time. The default price of USDC and USDT in DEX is 1, which is not affected by the fluctuation of the exchange. Currently, this strategy is basically adopted for on-chain data acquisition.

4. CONCLUSION

In this audit, we thoroughly analyzed **Tesa** Extension implementation. The problems found are described and explained in detail in Section 3. The problems found in the audit have been communicated to the project leader. We therefore consider the audit result to be Passed. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

5. APPENDIX

5.1 Basic Coding Assessment

5.1.1 Apply Verification Control

- Description: The security of apply verification
- Result: Not found
- Severity: Critical

5.1.2 Authorization Access Control

- Description: Permission checks for external integral functions
- Result: Not found
- Severity: Critical

5.1.3 Forged Transfer Vulnerability

- Description: Assess whether there is a forged transfer notification vulnerability in the contract
- Result: Not found
- Severity: Critical

5.1.4 Transaction Rollback Attack

- Description: Assess whether there is transaction rollback attack vulnerability in the contract.
- Result: Not found
- Severity: Critical

5.1.5 Transaction Block Stuffing Attack

- Description: Assess whether there is transaction blocking attack vulnerability.
- Result: Not found
- Severity: Critical

5.1.6 Soft Fail Attack Assessment

- Description: Assess whether there is soft fail attack vulnerability.
- Result: Not found
- Severity: Critical

5.1.7 Hard Fail Attack Assessment

- Description: Examine for hard fail attack vulnerability
- Result: Not found
- Severity: Critical

5.1.8 Abnormal Memo Assessment

- Description: Assess whether there is abnormal memo vulnerability in the contract.
- Result: Not found
- Severity: Critical

5.1.9 Abnormal Resource Consumption

- Description: Examine whether abnormal resource consumption in contract processing.
- Result: Not found
- Severity: Critical

5.1.10 Random Number Security

- Description: Examine whether the code uses insecure random number.
- Result: Not found
- Severity: Critical

5.2 Advanced Code Scrutiny

5.2.1 Cryptography Security

- Description: Examine for weakness in cryptograph implementation.
- Results: Not Found
- Severity: High

5.2.2 Account Permission Control

- Description: Examine permission control issue in the contract
- Results: Not Found
- Severity: Medium

5.2.3 Malicious Code Behavior

- Description: Examine whether sensitive behavior present in the code
- Results: Not found
- Severity: Medium

5.2.4 Sensitive Information Disclosure

- Description: Examine whether sensitive information disclosure issue present in the code.
- Result: Not found
- Severity: Medium

5.2.5 System API

- Description: Examine whether system API application issue present in the code
- Results: Not found
- Severity: Low

6. DISCLAIMER

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 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 without ExVul's prior written consent.

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 ExVul 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. ExVul's position is that each company and individual are responsible for their own due diligence and continuous security. ExVul'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.

7. REFERENCES

[1] MITRE. CWE- 191: Integer Underflow (Wrap or Wraparound).

https://cwe.mitre.org/data/ definitions/191.html.

[2] MITRE. CWE- 197: Numeric Truncation Error.

https://cwe.mitre.org/data/definitions/197. html.

[3] MITRE. CWE-400: Uncontrolled Resource Consumption.

https://cwe.mitre.org/data/ definitions/400.html.

[4] MITRE. CWE-440: Expected Behavior Violation.

https://cwe.mitre.org/data/definitions/440. html.

[5] MITRE. CWE-684: Protection Mechanism Failure.

https://cwe.mitre.org/data/definitions/ 693.html.

[6] MITRE. CWE CATEGORY: 7PK - Security Features.

https://cwe.mitre.org/data/definitions/ 254.html.

[7] MITRE. CWE CATEGORY: Behavioral Problems.

https://cwe.mitre.org/data/definitions/438. html.

[8] MITRE. CWE CATEGORY: Numeric Errors.

https://cwe.mitre.org/data/definitions/189.html.

[9] MITRE. CWE CATEGORY: Resource Management Errors.

https://cwe.mitre.org/data/ definitions/399.html.

[10] OWASP. Risk Rating Methodology.

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

www.exvul.com

contact@exvul.com

@EXVULSEC

github.com/EXVUL-Sec

ExVul