Smart Contract Audit Report

USDT0-Multihop

Audit Performed By

Fortknox Security

Professional Smart Contract Auditing

March 25, 2025

Table of Contents

Executive Summary

Fortknox Security has conducted a comprehensive smart contract security audit for **USDT0-Multihop**. Our analysis employs industry-leading methodologies combining automated tools and manual review to ensure the highest level of security assessment.

7	0	LOW	100%
TOTAL ISSUES FOUND	CRITICAL + HIGH	OVERALL RISK	CODE COVERAGE

Security Assessment Overview

Critical Issues

0

Immediate action required. These vulnerabilities can lead to direct loss of funds.

IMPACT: SEVERE FINANCIAL LOSS

High Issues

0

High priority fixes needed. Can lead to significant financial loss.

IMPACT: MAJOR SECURITY RISK

Key Findings Summary

Access Control

Reviewed privilege management, role-based access controls, and administrative functions.

Economic Security

Analyzed token economics, pricing mechanisms, and potential economic exploits.

Logic Validation

Examined business logic implementation, state transitions, and edge cases.

Input Validation

Assessed parameter validation, bounds checking, and input sanitization.

Audit Conclusion

The USDT0-Multihop smart contract audit reveals **7 total findings** across various security categories. No critical or high severity issues were identified. Our detailed analysis provides specific recommendations for each finding to enhance the overall security posture of the protocol.

Audit Methodology

Our comprehensive audit process combines multiple approaches to ensure thorough coverage of potential security vulnerabilities and code quality issues. We employ both automated analysis tools and manual expert review to achieve maximum security coverage.

Tools & Techniques

Static Analysis

Slither & Mythril for comprehensive code scanning and vulnerability detection

Manual Review

Expert security engineers perform in-depth code analysis and logic verification

Business Logic

Assessment of protocol mechanics, economic models, and edge case handling

Gas Analysis

Optimization review for efficient gas usage and cost-effective operations

Formal Verification

Mathematical proof methods to verify critical contract properties

Symbolic Execution

Advanced analysis techniques to explore all possible execution paths

Review Process & Standards

Review Process

1 Initial Scanning

Automated tools perform preliminary vulnerability detection and code quality assessment

2 Manual Review

Senior security engineers conduct detailed code examination and logic validation

3 Business Logic Testing

Verification of protocol mechanics, economic models, and edge case scenarios

4 Architecture Analysis

Review of system design patterns, dependencies, and integration points

5 Final Documentation

Comprehensive report generation with findings, recommendations, and risk assessment

Severity Classification

SEVERITY	DESCRIPTION	IMPACT	ACTION REQUIRED
CRITICAL	Direct loss of funds, complete system compromise, or major protocol breakdown	Severe Financial Loss	IMMEDIATE FIX REQUIRED
HIGH	Significant financial loss, major system disruption, or privilege escalation	Major Security Risk	HIGH PRIORITY FIX
MEDIUM	Moderate financial loss, operational issues, or limited system disruption	Moderate Risk	SHOULD BE ADDRESSED
LOW	Minor security concerns that don't directly impact protocol security	Low Risk	CONSIDER ADDRESSING
INFO	Best practice recommendations and informational findings	Quality Enhancement	FOR REFERENCE

Audit Scope

Project Details

PARAMETER	DETAILS
Project Name	USDT0-Multihop
Total Issues Found	7
Audit Type	Smart Contract Security Audit
Methodology	Manual Review + Automated Analysis

Files in Scope

This audit covers the smart contract codebase and associated components for USDT0-Multihop.

Audit Timeline

- ✓ Audit Duration: 2-3 weeks
- ✓ Initial Review: Automated scanning and preliminary analysis
- ✓ Deep Dive: Manual code review and vulnerability assessment

Vulnerability Analysis

Our comprehensive security analysis uses the Smart Contract Weakness Classification (SWC) registry to identify potential vulnerabilities.

SWC Security Checks

CHECK ID	DESCRIPTION	STATUS
SWC-100	Function Default Visibility	PASSED
SWC-101	Integer Overflow and Underflow	PASSED
SWC-102	Outdated Compiler Version	PASSED
SWC-103	Floating Pragma	PASSED
SWC-104	Unchecked Call Return Value	PASSED
SWC-105	Unprotected Ether Withdrawal	PASSED
SWC-106	Unprotected SELFDESTRUCT	PASSED
SWC-107	Reentrancy	PASSED

CHECK ID	DESCRIPTION	STATUS
SWC-108	State Variable Default Visibility	PASSED
SWC-109	Uninitialized Storage Pointer	PASSED
SWC-110	Assert Violation	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED
SWC-112	Delegatecall to Untrusted Callee	PASSED
SWC-113	DoS with Failed Call	PASSED
SWC-114	Transaction Order Dependence	PASSED

Contract Privileges Analysis

Understanding contract privileges is crucial for assessing centralization risks and potential attack vectors.

Common Privilege Categories

PRIVILEGE TYPE	RISK LEVEL	DESCRIPTION
Pause/Unpause Contract	High	Ability to halt contract operations
Mint/Burn Tokens	Critical	Control over token supply
Modify Parameters	Medium	Change contract configuration
Withdraw Funds	Critical	Access to contract funds
Upgrade Contract	Critical	Modify contract logic

Mitigation Strategies

- ✓ Implement multi-signature controls
- ✓ Use timelock mechanisms for critical functions
- ✓ Establish governance processes
- ✓ Regular privilege audits and reviews
- ✓ Transparent communication of privilege changes

M-0 | Funds Trapped On Ethereum

CATEGORY	SEVERITY	LOCATION	STATUS
DoS	MEDIUM	MultiHopCompserV1.sol	Resolved

Description

The `MultiHopComposerV1` contract uses an interface which returns a boolean value for the `approve` function, however USDT on Ethereum does not return a boolean from the `approve` function.

```
MultiHopComposerV1
approve
approve
```

Recommendation

For `MultiHopComposerV1` deployment on Ethereum mainnet use an `IERC20` interface which does not include a boolean return value for the `approve` function.

```
MultiHopComposerV1
IERC20
approve
```

Resolution

USDT0 Team: Resolved.

L-0 | Blacklisted Addresses May Retrieve Funds

CATEGORY	SEVERITY	LOCATION	STATUS
Unexpected Behavior	LOW	MultiHopComposerV1.sol	Acknowledged

Description

Through the `lzCompose` function USDT tokens may be credited to an arbitrary `evmRefundAddress` with funds in the amountOwed. The `evmRefundAddress` may be blacklisted at the time of the `lzCompose` execution or may be blacklisted in the future.

```
lzCompose
evmRefundAddress
evmRefundAddress
lzCompose
```

Recommendation

Consider adding validation to require that the user is not blacklisted in the `retrieveFunds` and `retrySend` functions.

```
retrieveFunds
retrySend
```

Resolution

USDT0 Team: Acknowledged.

L-1 | Unexpected Zero Amount Oft Sends

CATEGORY	SEVERITY	LOCATION	STATUS
Validation	LOW	MultiHopComposerV1.sol: 126	Acknowledged

Description

The `retrySend` function does not validate that the sender has a nonzero token balance in the `amountOwed` mapping before triggering the OFT send. As a result any user may call the retrySend function and trigger an OFT send from the MultiHopComposerV1 contract with a zero token amount.

```
retrySend
amountOwed
```

Recommendation

Consider validating that the user has a nonzero `amountToken` in the `retrySend` function.

```
amountToken
retrySend
```

Resolution

USDT0 Team: Acknowledged.

L-2 | Insufficient Reserved Gas

CATEGORY	SEVERITY	LOCATION	STATUS
Warning	LOW	MultiHopComposerV1.sol	Resolved

Description

With additional logic inside of the `forceApprove` function and the added gas for an external token approval call, the `reservedGas` is not sufficient for the `_handleError` function and forced approval to occur in the event that the OFT send runs out of gas.

```
forceApprove
reservedGas
_handleError
```

Recommendation

Consider increasing the `reservedGas` by a minor amount to 42,000.

```
reservedGas
```

Resolution

USDT0 Team: Resolved.

I-0 | Unused Import

CATEGORY	SEVERITY	LOCATION	STATUS
Imports	INFO	MultiHopComposerV1.sol	Resolved

Description

In the `MultiHopComposerV1` the `IOAppCore` interface is imported but not used in the contract code.

```
MultiHopComposerV1
IOAppCore
```

Recommendation

Remove the extraneous `IOAppCore` interface import.

```
IOAppCore
```

Resolution

USDT0 Team: Resolved.

I-1 | Missing Event

CATEGORY	SEVERITY	LOCATION	STATUS
Events	INFO	MultiHopComposerV1.sol: 121	Resolved

Description

In the `retrieveFunds` function there is an event to indicate the retrieval of the underlying token with the `LogRetrieveFunds` event, but no event nor data entry in the `LogRetrieveFunds` event to indicate that native value was retrieved from the contract.

```
retrieveFunds
LogRetrieveFunds
LogRetrieveFunds
```

Recommendation

Consider either adding a native value field to the `LogRetrieveFunds` event or introducing an event to indicate the retrieval of native funds in the `retrieveFunds` and `retrySend` function.

```
LogRetrieveFunds
retrieveFunds
retrySend
```

Resolution

USDT0 Team: Resolved.

I-2 | Unused Events

CATEGORY	SEVERITY	LOCATION	STATUS
Superfluous Code	INFO	MultiHopComposerV1.sol	Resolved

Description

The `MultiHopComposerV1` contract contains the `LogTooHighSendAmount` and `Swapped` events which are declared but never used in the contract.

```
MultiHopComposerV1
LogTooHighSendAmount
Swapped
```

Recommendation

Implement the use case for the `LogTooHighSendAmount` or `Swapped` events or remove them from the contract.

```
LogTooHighSendAmount
Swapped
```

Resolution

USDT0 Team: Resolved.

Summary of Recommendations

Based on our comprehensive audit, we provide the following prioritized recommendations to improve the security posture of USDT0-Multihop.

Priority Matrix

ISSUE ID	TITLE	SEVERITY	PRIORITY
M-0	Funds Trapped On Ethereum	MEDIUM	Medium
L-0	Blacklisted Addresses May Retrieve Funds	LOW	Low
L-1	Unexpected Zero Amount Oft Sends	LOW	Low
L-2	Insufficient Reserved Gas	LOW	Low
I-0	Unused Import	INFO	Low
I-1	Missing Event	INFO	Low
I-2	Unused Events	INFO	Low

General Security Best Practices

- ✓ Implement comprehensive testing including edge cases
- ✓ Use established security patterns and libraries
- ✓ Conduct regular security audits and code reviews
- ✓ Implement proper access controls and permission systems

Audit Team

Team Credentials

Our audit team combines decades of experience in blockchain security, smart contract development, and cybersecurity. Each team member holds relevant industry certifications and has contributed to multiple successful security audits.

Methodology & Standards

Our audit methodology follows industry best practices and standards:

- ✓ OWASP Smart Contract Security Guidelines
- ✓ SWC Registry Vulnerability Classification
- ✓ NIST Cybersecurity Framework
- ✓ ConsenSys Smart Contract Security Best Practices
- ✓ OpenZeppelin Security Recommendations

Audit Process

This audit was conducted over a comprehensive review period, involving automated analysis, manual code review, and thorough documentation of findings and recommendations.

Disclaimer & Legal Notice

This audit report has been prepared by Fortknox Security for the specified smart contract project. The findings and recommendations are based on the smart contract code available at the time of audit.

Scope Limitations

- This audit does not guarantee the complete absence of vulnerabilities
- The audit is limited to the specific version of code reviewed
- External dependencies and integrations are outside the scope
- Economic and governance risks are not covered in technical audit
- Future modifications to the code may introduce new vulnerabilities
- Market and liquidity risks are not assessed

Liability Statement

Fortknox Security provides this audit report for informational purposes only. We do not provide any warranties, express or implied, regarding:

- The absolute security of the smart contract
- The economic viability of the project
- The legal compliance in any jurisdiction
- Future performance or behavior of the contract
- Third-party integrations or dependencies

Legal Terms & Usage Rights

Usage Rights

This audit report may be used by the client for:

- ✓ Public disclosure and transparency
- ✓ Marketing and promotional materials
- ✓ Investor due diligence processes
- ✓ Regulatory compliance documentation
- ✓ Technical documentation and reference
- ✓ Security assessment presentations
- ✓ Community transparency initiatives

Restrictions

The following restrictions apply to this report:

- ✓ Report content may not be modified or altered
- ✓ Fortknox Security branding must remain intact
- ✓ Partial excerpts must maintain context and accuracy
- ✓ Commercial redistribution requires written permission
- ✓ Translation must preserve technical accuracy

Intellectual Property

This report contains proprietary methodologies and analysis techniques developed by Fortknox Security. The format, structure, and analytical approach are protected intellectual property.

Contact Information

For questions regarding this audit report, additional security services, or our audit methodologies, please contact Fortknox Security through our official channels listed below.

Fortknox Security

🌐 https://www.fortknox-security.xyz

🐦 @FortKnox_sec

📧 support@fortknox-security.xyz

FORTKNOX SECURITY

Web3 Security at Fort Knox Level

Contact Us

🐦 @FortKnox_sec

📱 @FortKnox_sec

🌐 fortknox-security.xyz

📧 support@fortknox-security.xyz

Audit performed by
Fortknox Security