SMART CONTRACT AUDIT REPORT

for

Chainhop

Prepared By: Xiaomi Huang

PeckShield

August 28, 2022

Document Properties

Client	ChainHop
Title	Smart Contract Audit Report
Target	Chainhop
Version	1.0
Author	Shulin Bie
Auditors	Shulin Bie, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	August 28, 2022	Shulin Bie	Final Release
1.0-rc	August 26, 2022	Shulin Bie	Release Candidate

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the `Chainhop`, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Chainhop

`Chainhop` implements a cross-chain decentralized exchange (`DEX`), which provides the cross-chain swap service with a one-transaction user experience. The audited changeset implements the multi-bridge aggregation, including `cBridge`, `Multichain`, and `Stargate`. It provides the user with unprecedented performance and flexibility.

Table 1.1: Basic Information of Chainhop

Item	Description
Target	Chainhop
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	August 28, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. Please note that this audit covers the following contracts: `TransferSwapper.sol`, `AnyswapAdapter.sol`, `CBridgeAdapter.sol`, `StargateAdapter.sol`, and `BridgeRegistry.sol`.

- https://github.com/chainhop-dex/chainhop-contracts.git (05c56f8)

And this is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/chainhop-dex/chainhop-contracts.git (68c2105)

1.2 About PeckShield

PeckShield Inc. [9] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [8]:

- 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 demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

deploy contracts on our private testnet 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 1.3.

In particular, we perform the audit according to the following procedure:

- 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.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.
- Advanced DeFi Scrutiny: 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.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [7], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the `Chainhop` implementation. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logic, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	■
Low	2	■ ■
Informational	0	
Total	3	

We have previously audited the main `Chainhop` protocol. In this report, we exclusively focus on the specific changeset `(0969d42..05c56f8)`, we determine three issues that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussion of the issues are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerability and 2 low-severity vulnerabilities.

Table 2.1: Key Chainhop Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Improved Logic of TransferSwapper::transferWithSwap()	Business Logic	Fixed
PVE-002	Low	Accommodation Of Non-ERC20-Compliant Tokens	Coding Practices	Fixed
PVE-003	Medium	Trust Issue Of Admin Keys	Security Features	Confirmed

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 Detailed Results

3.1 Improved Logic of TransferSwapper::transferWithSwap()

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: TransferSwapper
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

The Chainhop protocol implements a cross-chain decentralized exchange (DEX) and multi-bridge aggregation (including cBridge, Multichain, and Stargate). It allows the user to swap one token to another on the source chain via the user specified DEXes and then cross the swapped-out token to the destination chain. On the destination chain, the bridge token can be further swapped to the user expected token via the user specified DEXes. Additionally, it implements a so-called forward feature, which allows the cross-chain assets to be further forwarded from the destination chain to another chain. In particular, one entry routine, i.e., transferWithSwap(), is designed to trigger the cross-chain transaction. While examining its logic, we notice the current implementation needs to be improved.

To elaborate, we show below the related code snippet of the TransferSwapper contract. Considering only the cBridge supports the cross-chain swap service, the statement of `require(_dstSwaps.length == 0 || bridgeProviderHash == CBRIDGE_PROVIDER_HASH, "bridge does not support msg")` (line 135) is executed to meet the requirement. However, it ignores the fact that the forward feature can only be supported by cBridge as well. Given this, we suggest to improve the implementation as below: `require((_dstSwaps.length == 0 && _desc.forward.length == 0)|| bridgeProviderHash == CBRIDGE_PROVIDER_HASH, "bridge does not support msg")` (line 135).

```
125     function transferWithSwap(
126         Types.TransferDescription calldata _desc,
127         ICodec.SwapDescription[] calldata _srcSwaps,
128         ICodec.SwapDescription[] calldata _dstSwaps
129     ) external payable nonReentrant {
```

```
        // a request needs to incur a swap, a transfer, or both. otherwise it's a nop and we revert early to save gas
        require(_srcSwaps.length != 0  _desc.dstChainId != uint64(block.chainid), "nop");
        require(_srcSwaps.length != 0  (_desc.amountIn != 0 && _desc.tokenIn != address(0)), "nop");
        // swapping on the dst chain requires message passing. only integrated with cbridge for now
        bytes32 bridgeProviderHash = keccak256(bytes(_desc.bridgeProvider));
        require(_dstSwaps.length == 0  bridgeProviderHash == CBRIDGE_PROVIDER_HASH, "bridge does not support msg");

        IBridgeAdapter bridge = bridges[bridgeProviderHash];
        // if not DirectSwap, the bridge provider should be a valid one
        require(_desc.dstChainId == uint64(block.chainid)  address(bridge) != address(0), "unsupported bridge");

        uint256 amountIn = _desc.amountIn;
        ICodec[] memory codecs;

        address srcToken = _desc.tokenIn;
        address bridgeToken = _desc.tokenIn;
        if (_srcSwaps.length != 0) {
            (amountIn, srcToken, bridgeToken, codecs) = sanitizeSwaps(_srcSwaps);
        }
        if (_desc.nativeIn) {
            require(srcToken == nativeWrap, "tkin no nativeWrap");
            require(msg.value >= amountIn, "insfcnt amt"); // insufficient amount
            IWETH(nativeWrap).deposit{value: amountIn}();
        } else {
            IERC20(srcToken).safeTransferFrom(msg.sender, address(this), amountIn);
        }

        _swapAndSend(srcToken, bridgeToken, amountIn, _desc, _srcSwaps, _dstSwaps, codecs);
    }
```

Listing 3.1: `TransferSwapper::transferWithSwap()`

Note another routine, i.e., `_transfer()`, shares the similar issue.

Recommendation Improved the implementation of the `transferWithSwap()` and `_transfer()` routines as above-mentioned.

Status The issue has been addressed by the following commit: `09b2e68`.

3.2 Accommodation Of Non-ERC20-Compliant Tokens

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `Multiple Contracts`
- Category: Coding Practices [5]
- CWE subcategory: CWE-1109 [1]

Description

Though there is a standardized ERC-20 specification, many token contracts may not strictly follow the specification or have additional functionalities beyond the specification. In this section, we examine the `transferFrom()` routine and possible idiosyncrasies from current widely-used token contracts.

In particular, we use the popular token, i.e., `ZRX`, as our example. We show the related code snippet below. On its entry of `transferFrom()`, there is a check, i.e., `if (balances[_from] >= _value && allowed[_from][msg.sender] >= _value && balances[_to] + _value >= balances[_to])`. If the check fails, it returns `false`. However, the transaction still proceeds successfully without being reverted. This is not compliant with the ERC20 standard and may cause issues if not handled properly. Specifically, the ERC20 standard specifies the following: *"Transfers _value amount of tokens from address _from to address _to, and MUST fire the Transfer event. The function SHOULD throw unless the _from account has deliberately authorized the sender of the message via some mechanism."*

```
    function transfer(address _to, uint _value) returns (bool) {
        //Default assumes totalSupply can't be over max (2^256 - 1).
        if (balances[msg.sender] >= _value && balances[_to] + _value >= balances[_to]) {
            balances[msg.sender] -= _value;
            balances[_to] += _value;
            Transfer(msg.sender, _to, _value);
            return true;
        } else { return false; }
    }

    function transferFrom(address _from, address _to, uint _value) returns (bool) {
        if (balances[_from] >= _value && allowed[_from][msg.sender] >= _value &&
            balances[_to] + _value >= balances[_to]) {
            balances[_to] += _value;
            balances[_from] -= _value;
            allowed[_from][msg.sender] -= _value;
            Transfer(_from, _to, _value);
            return true;
        } else { return false; }
    }
```

Listing 3.2: `ZRX.sol`

Because of that, a normal call to `transferFrom()` is suggested to use the safe version, i.e., `safeTransferFrom()`. In essence, it is a wrapper around ERC20 operations that may either throw on failure or return false without reverts. Moreover, the safe version also supports tokens that return no value (and instead revert or throw on failure). Note that non-reverting calls are assumed to be successful. Similarly, there is a safe version of `approve()` as well, i.e., `safeApprove()`.

In the following, we show the related code snippet of the `TransferSwapper` contract. If the `USDT` token is supported as `_token`, the unsafe version of `IERC20(_token).transferFrom(msg.sender, address(this), _amount)` (line 371) may revert as there is no return value in the `USDT` token contract's `transferFrom()` implementation (but the `IERC20` interface expects a return value). We may intend to replace `IERC20(_token).transferFrom(msg.sender, address(this), _amount)` (line 371) with `safeTransferFrom()`.

```
365     function executeMessageWithTransferRefundFromAdapter(
366         address _token,
367         uint256 _amount,
368         bytes calldata _message,
369         address // _executor
370     ) external nonReentrant returns (ExecutionStatus) {
371         IERC20(_token).transferFrom(msg.sender, address(this), _amount);
372         return _refund(_token, _amount, _message);
373     }
374 }
```

Listing 3.3: `TransferSwapper::executeMessageWithTransferRefundFromAdapter()`

Note that the other routines, i.e., `AnyswapAdapter::bridge()`, `CBridgeAdapter::bridge()`, and `Stargate-Adapter::bridge()`, can be similarly improved.

Recommendation Accommodate the above-mentioned idiosyncrasy with safe-version implementation of ERC20-related `transferFrom()` and `approve()`. And there is a need to `approve()` twice: the first one reduces the allowance to 0; and the second one sets the new allowance.

Status The issue has been addressed by the following commit: `09b2e68`.

3.3 Trust Issue Of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [2]

Description

In the `Chainhop` implementation, there is a privileged account that plays a critical role in governing and regulating the protocol-wide operations (e.g., configuring various system parameters). In the following, we show the representative functions potentially affected by the privilege of the account.

```
    function updateMainContract(address _mainContract) external onlyOwner {
        mainContract = _mainContract;
        emit MainContractUpdated(_mainContract);
    }

    function setSupportedRouter(address _router, bool _enabled) external onlyOwner {
        bool enabled = supportedRouters[_router];
        require(enabled != _enabled, "nop");
        supportedRouters[_router] = _enabled;
        emit SupportedRouterUpdated(_router, _enabled);
    }
```

Listing 3.4: `AnyswapAdapter::updateMainContract()&&setSupportedRouter()`

We emphasize that the privilege assignment is indeed necessary and consistent with the protocol design. However, it will be worrisome if the privileged account is a plain EOA account. A multi-sig account could greatly alleviate this concern, though it is still far from perfect. Note that a compromised privileged account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

Recommendation Suggest a multi-sig account plays the privileged `owner` account to mitigate this issue. Additionally, all changes to privileged operations may need to be mediated with necessary timelocks.

Status The issue has been confirmed by the team.

4 Conclusion

In this audit, we have analyzed the design and implementation of the `Chainhop` protocol, which implements a cross-chain decentralized exchange (`DEX`), which provides the cross-chain swap service with a one-transaction user experience. Additionally, it implements the multi-bridge aggregation, including `cBridge`, `Multichain`, and `Stargate`. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

[4] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[5] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[6] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[7] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[8] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[9] PeckShield. PeckShield Inc. https://www.peckshield.com.