



Security Assessment

SuperSwap

Verified on 3/30/25

SUMMARY

Project

SuperSwap

CHAIN

Base

METHODOLOGY

Manual & Automatic Analysis

FILES

Single

DELIVERY

3/30/25

TYPE

Standard Audit



Total Findings

Critical

Major

Medium

Minor

Informational

Resolved

 1 Critical

An exposure that can affect the contract functions in several events that can risk and disrupt the contract

 0 Major


An opening & exposure to manipulate the contract in an unwanted manner

 0 Medium

An opening that could affect the outcome in executing the contract in a specific situation

 0 Minor

An opening but doesn't have an impact on the functionality of the contract

 1 Informational

An opening that consists information but will not risk or affect the contract

 2 Resolved

ContractWolf's findings has been acknowledged & resolved by the project

STATUS
 **AUDIT PASSED**

TABLE OF CONTENTS | SuperSwap

| Summary

- Project Summary
- Findings Summary
- Disclaimer
- Scope of Work
- Auditing Approach

| Project Information

- Token/Project Details
- Inheritance Graph
- Call Graph

| Findings

- Issues
- SWC Attacks
- CW Assessment
- Fixes & Recommendation
- Audit Comments

DISCLAIMER | SuperSwap

ContractWolf audits and reports should not be considered as a form of project's "Advertisement" and does not cover any interaction and assessment from "Project Contract" to "External Contracts" such as PancakeSwap, UniSwap, SushiSwap or similar.

ContractWolf does not provide any warranty on its released report and should not be used as a decision to invest into audited projects.

ContractWolf provides a transparent report to all its "Clients" and to its "Clients Participants" and will not claim any guarantee of bug-free code within its **SMART CONTRACT**.

ContractWolf's presence is to analyze, audit and assess the Client's Smart Contract to find any underlying risk and to eliminate any logic and flow errors within its code.

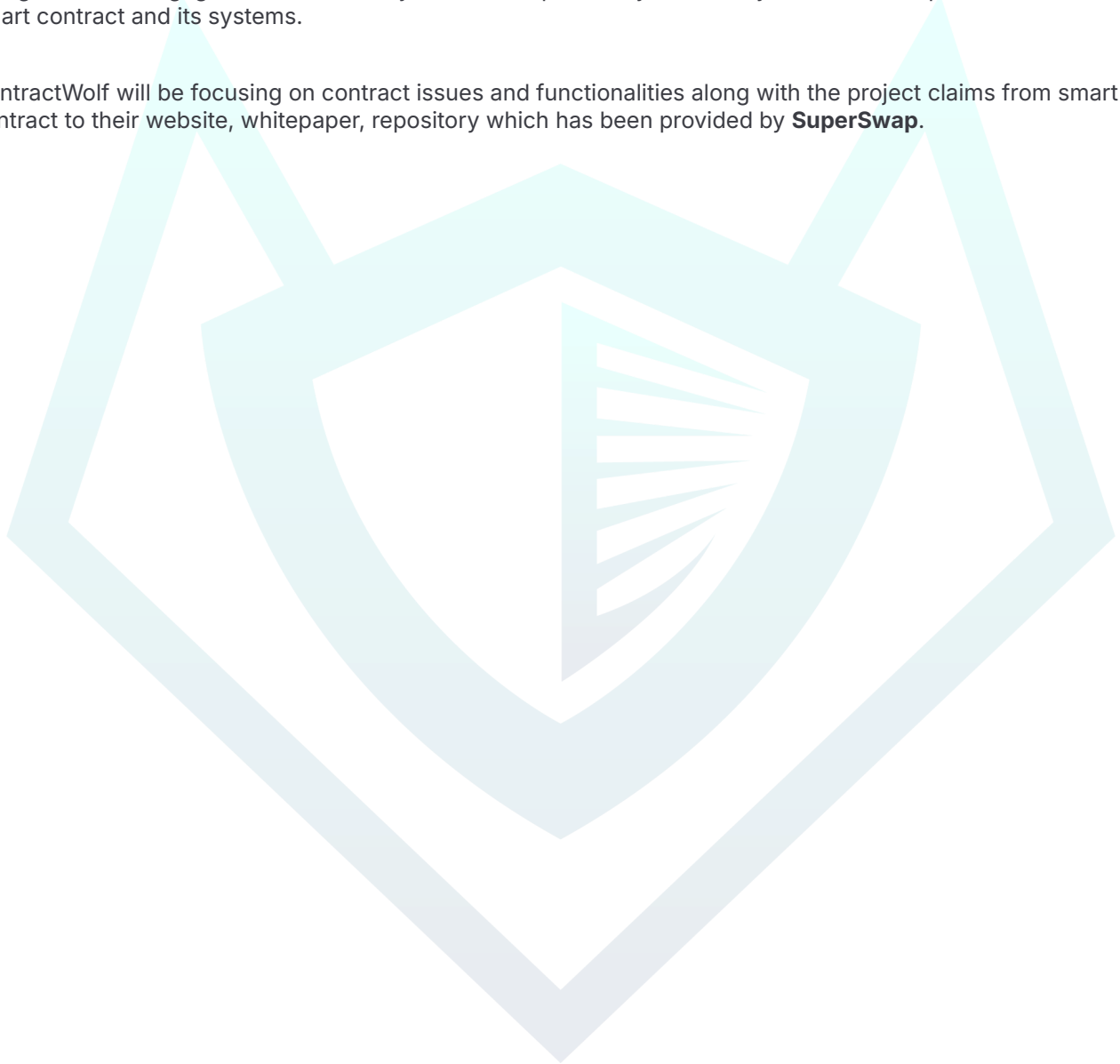
Each company or project should be liable to its security flaws and functionalities.

SCOPE OF WORK | SuperSwap

SuperSwap team has agreed and provided us with the files that need to be tested (*Github, BSCscan, Etherscan, Local files etc*). The scope of audit is the main contract.

The goal of this engagement is to identify if there is a possibility of security flaws in the implementation of smart contract and its systems.

ContractWolf will be focusing on contract issues and functionalities along with the project claims from smart contract to their website, whitepaper, repository which has been provided by **SuperSwap**.



AUDITING APPROACH | SuperSwap

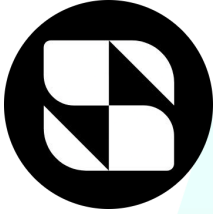
Every line of code along with its functionalities will undergo manual review to check for security issues, quality of logic and contract scope of inheritance. The manual review will be done by our team that will document any issues that they discovered.

METHODOLOGY

The auditing process follows a routine series of steps :

1. Code review that includes the following :
 - Review of the specifications, sources and instructions provided to ContractWolf to make sure we understand the size, scope and functionality of the smart contract.
 - Manual review of code. Our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities, underlying and hidden security flaws.
2. Testing and automated analysis that includes :
 - Testing the smart contract function with common test cases and scenarios to ensure that it returns the expected results.
3. Best practices and ethical review. The team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security and control within the smart contract.
4. Recommendations to help the project take steps to eliminate or minimize threats and secure the smart contract.

TOKEN DETAILS | SuperSwap



Cross chain swaps

Token Name

-

Symbol

-

Decimal

-

Total Supply

-

Chain

Base

SOURCE

Source

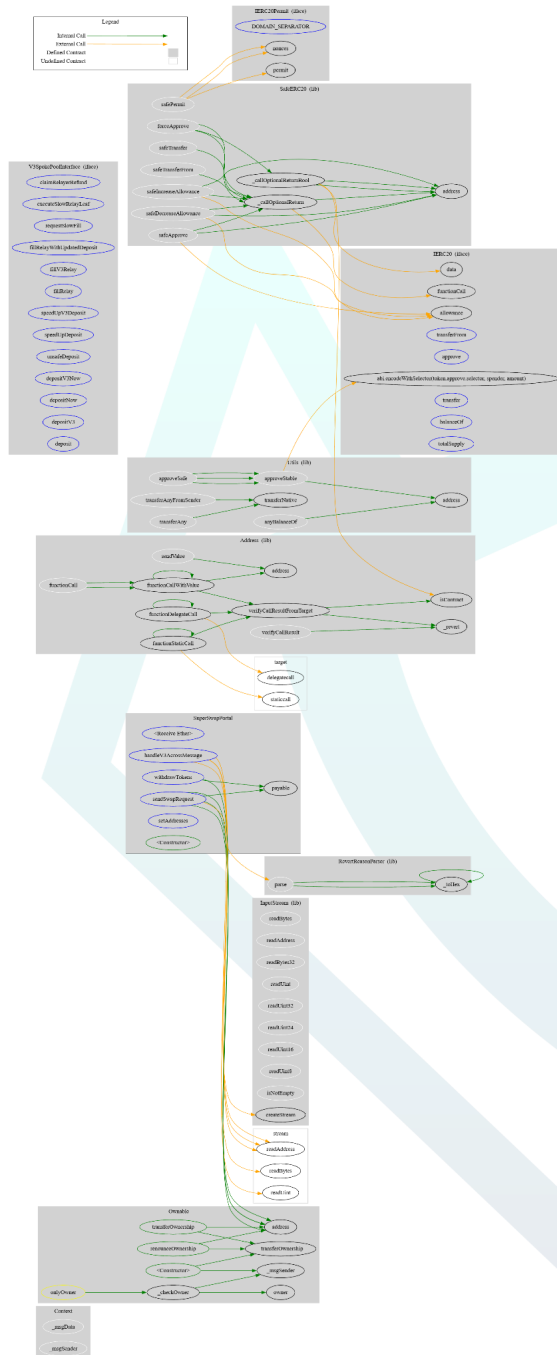
Base - 0x7b92d0ceA18F5598fC560F24f8948740D1eA833C
Ink - 0x51d3f0ecd9fd194eB3cF3aB177241AfEcE4d5494

INHERITANCE GRAPH | SuperSwap

Inheritance Graph of Contract Functions



Call Graph of Contract Functions



FINDINGS | SuperSwap



Total Findings

Critical

Major

Medium

Minor

Informational

Resolved

This report has been prepared to state the issues and vulnerabilities for SuperSwap through this audit. The goal of this report findings is to identify specifically and fix any underlying issues and errors

ID	Title	File & Line #	Severity	Status
SWC-107	Reentrancy Attack	SuperSwap.sol	Critical	● Resolved
SWC-105	Unprotected Ether Withdrawal	SuperSwap.sol	Critical	● Resolved
SWC-107	Reentrancy Attack	SuperSwap.sol	Critical	● Pending
SWC-103	Floating Pragma is set	SuperSwap.sol	Informational	● Pending

SWC ATTACKS | SuperSwap

Smart Contract Weakness Classification and Test Cases

ID	Description	Status
SWC-100	Function Default Visibility	● Passed
SWC-101	Integer Overflow and Underflow	● Passed
SWC-102	Outdated Compiler Version	● Passed
SWC-103	FloatingPragma	● Not Passed
SWC-104	Unchecked Call Return Value	● Passed
SWC-105	Unprotected Ether Withdrawal	● Passed
SWC-106	Unprotected SELF DESTRUCT Instruction	● Passed
SWC-107	Reentrancy	● Critical
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
SWC-115	Authorization through tx.origin	● Passed
SWC-116	Block values as a proxy for time	● Passed
SWC-117	Signature Malleability	● Passed
SWC-118	Incorrect Constructor Name	● Passed
SWC-119	Shadowing State Variables	● Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	● Passed
SWC-121	Missing Protection against Signature Replay Attacks	● Passed
SWC-122	Lack of Proper Signature Verification	● Passed

ID	Description	Status
SWC-123	Requirement Violation	● Passed
SWC-124	Write to Arbitrary Storage Location	● Passed
SWC-125	Incorrect Inheritance Order	● Passed
SWC-126	Insufficient Gas Griefing	● Passed
SWC-127	Arbitrary Jump with Function Type Variable	● Passed
SWC-128	DoS With Block Gas Limit	● Passed
SWC-129	Typographical Error	● Passed
SWC-130	Right-To-Left-Override control character(U+202E)	● Passed
SWC-131	Presence of unused variables	● Passed
SWC-132	Unexpected Ether balance	● Passed
SWC-133	Hash Collisions With Multiple Variable Arguments	● Passed
SWC-134	Message call with hardcoded gas amount	● Passed
SWC-135	Code With No Effects	● Passed
SWC-136	Unencrypted Private Data On-Chain	● Passed

CW ASSESSMENT | SuperSwap

ContractWolf Vulnerability and Security Tests

ID	Name	Description	Status
CW-001	Multiple Version	Presence of multiple compiler version across all contracts	✓
CW-002	Incorrect Access Control	Additional checks for critical logic and flow	✓
CW-003	Payable Contract	A function to withdraw ether should exist otherwise the ether will be trapped	✓
CW-004	Custom Modifier	major recheck for custom modifier logic	✓
CW-005	Divide Before Multiply	Performing multiplication before division is generally better to avoid loss of precision	✓
CW-006	Multiple Calls	Functions with multiple internal calls	✓
CW-007	Deprecated Keywords	Use of deprecated functions/operators such as block.blockhash() for blockhash(), msg.gas for gasleft(), throw for revert(), sha3() for keccak256(), callcode() for delegatecall(), suicide() for selfdestruct(), constant for view or var for actual type name should be avoided to prevent unintended errors with newer compiler versions	✓
CW-008	Unused Contract	Presence of an unused, unimported or uncalled contract	✓
CW-009	Assembly Usage	Use of EVM assembly is error-prone and should be avoided or double-checked for correctness	✓
CW-010	Similar Variable Names	Variables with similar names could be confused for each other and therefore should be avoided	✓
CW-011	Commented Code	Removal of commented/unused code lines	✓
CW-012	SafeMath Override	SafeMath is no longer needed starting with Solidity v0.8+. The compiler now has built-in overflow checking.	✓

FIXES & RECOMMENDATION

SWC-103 | A Floating Pragma is Set

Using a floating Solidity version (^) allows the contract to be compiled with future compiler versions that may introduce unintended behavior.

```
pragma solidity ^0.8.10;
```

Recommendation

Lock the compiler to a specific version to ensure consistent and auditable behavior.

```
pragma solidity 0.8.19;
```

SWC-105 | Unprotected Ether or Token Withdrawal

A function allows token transfers to arbitrary recipients without validating the caller, making it vulnerable to unauthorized withdrawals.

```
function handleV3AcrossMessage(...) external payable {  
    ...  
    IERC20(WETH).safeTransfer(recipient, amount); // Can be called by anyone  
    ...  
}
```

Recommendation

Restrict this function to be callable only by a trusted source

```
require(msg.sender == spokePoolAddress, "Unauthorized caller");
```

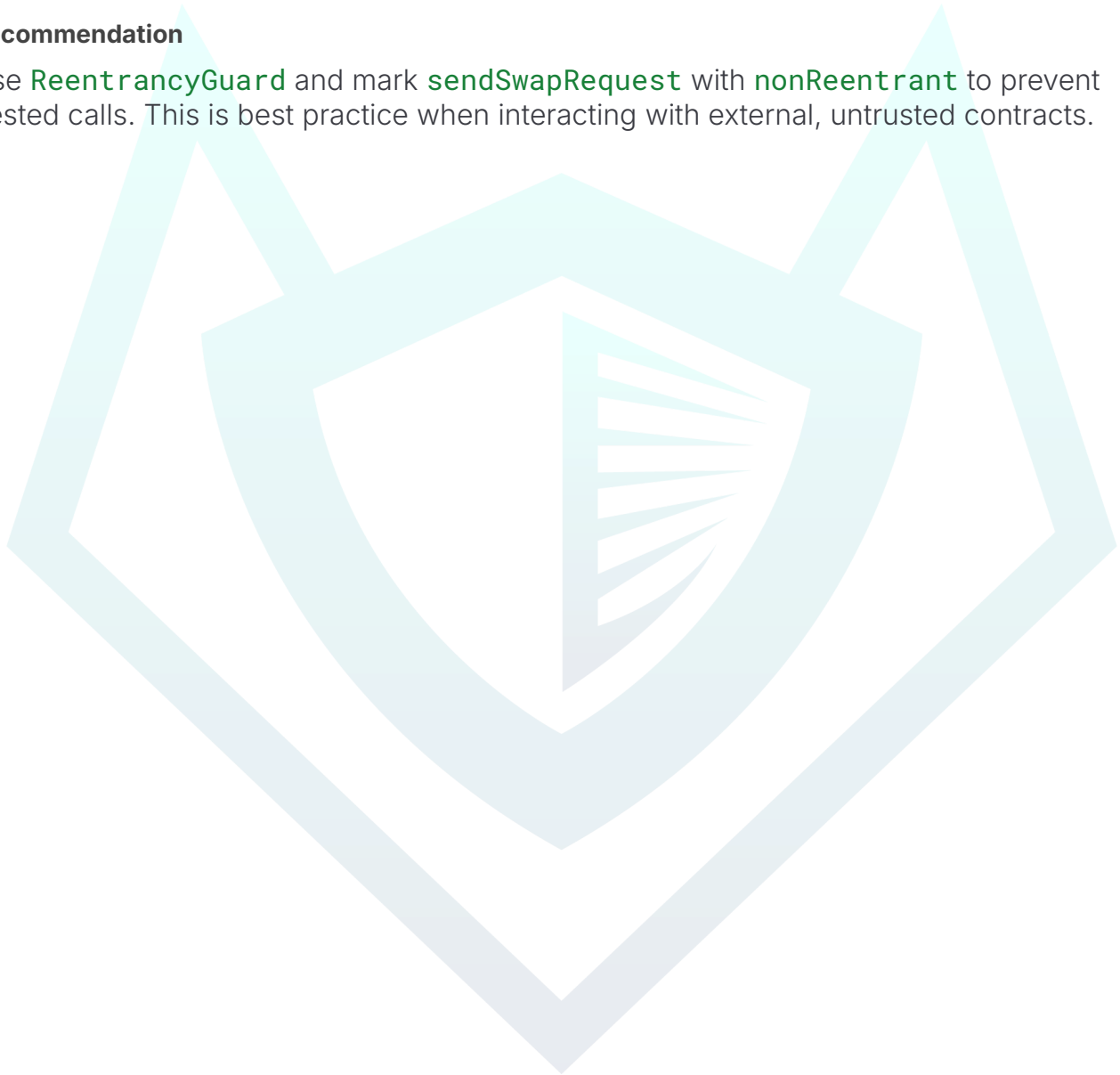
SWC-107 | Reentrancy

A function allows token transfers to arbitrary recipients without validating the caller, making it vulnerable to unauthorized withdrawals.

```
(bool success, bytes memory result) = payable(superSwapAddress)  
    .call{value: msg.value}(originData);
```

Recommendation

Use **ReentrancyGuard** and mark **sendSwapRequest** with **nonReentrant** to prevent nested calls. This is best practice when interacting with external, untrusted contracts.



SWC-107 | Reentrancy

The identified line allows arbitrary calls to `superSwapAddress` using user-provided `originData`, posing a significant risk if `superSwapAddress` is not entirely trusted.

Recommendation :

Sample code & logic :

```
// Before the external call, restrict the function selector.
bytes4 allowedSelector = bytes4(keccak256("swap(bytes)"));
require(bytes4(originData) == allowedSelector, "Invalid function");

// After a successful call, reset approval.
IERC20(tokenIn).forceApprove(superSwapAddress, 0);
```

you can change **"swap"** and derive the swap function of your choice, in this case lets use `swapExactTokensForTokens` for an example

```
bytes4 allowedSelector =
bytes4(keccak256("swapExactTokensForTokens(uint256,uint256,address[],address,uint256)"));
```

Other approach, longer and multiple validations :

```
if (originData.length > 0) {
  // Validate that the payload is long enough for a function selector (4 bytes)
  require(originData.length >= 4, "SuperSwapPortal: Payload too short");

  // Calculate expected function selector for the intended function
  bytes4 allowedSelector =
bytes4(keccak256("swapExactTokensForTokens(uint256,uint256,address[],address,uint256)"));

  // Extract the first 4 bytes (function selector) from the originData payload
  bytes4 actualSelector;
  assembly {
    actualSelector := mload(add(originData, 32))
  }
  // Validate that the actual selector matches the expected one
  require(actualSelector == allowedSelector, "SuperSwapPortal: Invalid payload
function selector");

  // After a successful call, reset approval.
  IERC20(tokenIn).forceApprove(superSwapAddress, 0);
}
```

AUDIT COMMENTS | SuperSwap

Smart Contract audit comment for a non-technical perspective

- Owner can update swap aggregator and bridge contract
- Owner can renounce and transfer ownership
- Owner can withdraw tokens and ETH from the contract
- Owner cannot mint after initial deployment
- Owner cannot burn
- Owner cannot pause contract
- Owner cannot block users
- Owner cannot update fees
- Owner cannot update max transaction amount



CONTRACTWOLF

Blockchain Security - Smart Contract Audits