BLOCK AUDIT REPORT

Smart Contract Security Audit Report

Smurfs INU

Block Audit Report Team received the SmurfsINU.sol file for smart contract security audit of the Smurfs INU on Aug 16, 2022. The following are the details and results of this smart contract security audit:

Project Name: Smurfs INU

The Contract address: 0x75aFA9915B2210Cd6329E820af0365e932bC1dd5

Link Address:
https://bscscan.com/address/0x75afa9915b2210cd6329e820af0365e932bc1dd5#code

The audit items and results:

(Other undiscovered security vulnerabilities are not included in the audit responsibility scope)

Audit Result: Passed

Audit Number: BAR0022116082022

Audit Date: Aug 16, 2022

Audit Team: Block Audit Report Team

Table of Content

Introduction

This Audit Report mainly focuses on the extensive security of Smurfs INU Smart Contract. With this report, we attempt to ensure the reliability and correctness of the smart contract by complete and rigorous assessment of the system's architecture and the smart contract codebase.

Auditing Approach and Methodologies applied

The Block Audit Report team has performed rigorous testing of the project including the analysis of the code design patterns where we reviewed the smart contract architecture to ensure it is structured along with the safe use of standard inherited contracts and libraries. Our team also conducted a formal line by line inspection of the Smart Contract i.e., a manual review, to find potential issues including but not limited to;

- Race conditions
- Zero race conditions approval attacks
- Re-entrancy
- Transaction-ordering dependence
- Timestamp dependence
- Check-effects-interaction pattern (optimistic accounting)
- Decentralized denial-of-service attacks
- Secure ether transfer pattern
- Guard check pattern
- Fail-safe mode
- Gas-limits and infinite loops
- Call Stack depth

In the Unit testing Phase, we coded/conducted custom unit tests written against each function in the contract to verify the claimed functionality from our client.
In Automated Testing, we tested the Smart Contract with our standard set of multifunctional tools to identify vulnerabilities and security flaws.
The code was tested in collaboration of our multiple team members and this included but not limited to;

- Testing the functionality of the Smart Contract to determine proper logic has been followed throughout the whole process.
- Analyzing the complexity of the code in depth and detailed, manual review of the code, line-by-line.
- Deploying the code on testnet using multiple clients to run live tests.
- Analyzing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analyzing the security of the on-chain data.

Audit Details

Project Name: Smurfs INU
Website/ BSCscan Code (Mainnet):
0x75aFA9915B2210Cd6329E820af0365e932bC1dd5

Languages: Solidity (Smart contract)
Platforms and Tools: Remix IDE, Truffle, Ganache, Mythril, Contract Library, Slither, Dapp. Tools, Echidna, Etheno

Audit Goals

The focus of the audit was to verify that the Smart Contract System is secure, resilient and working according to the specifications. The audit activities can be grouped in the following three categories:

Security Sight

Identifying security related issues within each contract and the system of contract.

Sound Architecture

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices, standard software design principle, design patterns and practices.

Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Usability vs Security
- Sections of code with high complexity
- Quantity and quality of test coverage

Issue Categories

Every issue in this report was assigned a severity level from the following:

Critical Severity Issues

Issues of this level are critical to the smart contract's performance/functionality and should be fixed before moving to a production environment.

High level severity issues

Issues on this level are strongly suggested by the team to be fixed before moving to the production environment.

Medium level severity issues

Issues on this level could potentially bring problems and should eventually be fixed.

Low level severity issues

Issues on this level are minor details and warning's that can remain unfixed but would be better fixed at some point in the future.

Issues Checking Status

№	Issue description	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Oracle calls.	Passed
4	Timestamp dependence.	Passed
5	DoS with Revert.	Passed
6	DoS with block gas limit.	Passed
7	Methods execution permissions.	Passed
8	Economy model.	Passed
9	The impact of the exchange rate on the logic.	Passed
10	Malicious Event log.	Passed
11	Scoping and Declarations.	Passed
12	Uninitialized storage pointers.	Passed
13	Arithmetic Operations accuracy.	Passed
14	Design Logic.	Passed
15	Cross-function race conditions.	Passed
16	Safe usage for Open Zeppelin module.	Passed
17	Fallback function security.	Passed
18	Send & receive ether.	Passed
19	Zero race condition approval attacks.	Passed
20	Short address attack.	Passed
21	Owner’s authority to freeze.	Passed
22	Attempt to block ether flows.	Passed
23	Redundant inheritance check.	Passed
24	Silent overrides of mapping structs.	Passed
25	Function state mutability.	Passed
26	Unnecessary conversion of type.	Passed

Used Code from other Framework/Smart Contracts (direct import)

- msgSender()

[+] interface IERC20

- totalSupply()
- balanceOf(address account)
- transfer(address recipient, ...
- allowance(address owner, add ...
- approve(address spender, uin ...
- transferFrom(

[+] contract Ownable is Context

- owner()
- transferOwnership(address ne ...

[+] library SafeMath

- add(uint256 a, uint256 b)
- sub(uint256 a, uint256 b)
- sub(
- mul(uint256 a, uint256 b)
- div(uint256 a, uint256 b)
- div(

[+] interface IUniswapV2Factory

- createPair(address tokenA, a ...

[+] interface IUniswapV2Router02

- swapExactTokensForETHSupport ...
- factory()
- WETH()
- addLiquidityETH(

[+] contract SmurfsINU is Context, IER ... *

- name()
- symbol()
- decimals()
- totalSupply()
- balanceOf(address account)
- transfer(address recipient, ...

- allowance(address owner, add ...
- approve(address spender, uin ...
- transferFrom(
- tokenFromReflection(uint256 ...
- removeAllFee()
- restoreAllFee()
- approve(
- transfer(
- swapTokensForEth(uint256 tok ...
- sendETHToFee(uint256 amount)
- manualswap()
- manualsend()
- smurfing(address[] memory sm ...
- gargamel(address notsmurf)
- tokenTransfer(
- transferStandard(
- takeTeam(uint256 tTeam)
- withdrawToken(address token ...
- reflectFee(uint256 rFee, ui ...
- getValues(uint256 tAmount)
- getTValues(
- getRValues(
- getRate()
- getCurrentSupply()
- excludeMultipleAccountsFromF ...

Manual Audit:

For this section the code was tested/read line by line by our auditors. We used Remix IDE's JavaScript VM and testnet Kovan to test the contract functionality in a simulated environment.

Started	Tue Aug 16 2022 08:39:31 GMT+0000 (Coordinated Universal Time)
Finished	Tue Aug 16 2022 08:39:40 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Remythx
Main Source File	SmurfsINU.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	1

Critical Severity Issues

No critical severity issues found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

Title – Floating Pragma		Location
SWC-103		
Relationships	CWE-664: Improper Control of a Resource Through its Lifetime	
Description	Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.	
Remediation	Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen. Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.	
Status	Acknowledged	

UNKNOWN Arithmetic operation "+" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file
SmurfsINU.sol
Locations

```
86 | library SafeMath {
87 | function add(uint256 a, uint256 b) internal pure returns (uint256) {
88 | uint256 c = a + b;
89 | require(c >= a, "SafeMath: addition overflow");
90 | return c;
```

UNKNOWN Arithmetic operation "-" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file
SmurfsINU.sol
Locations

```
101 | ) internal pure returns (uint256) {
102 | require(b <= a, errorMessage);
103 | uint256 c = a - b;
104 | return c;
105 | }
```

UNKNOWN Arithmetic operation "*" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
109 return 0;
110 }
111 uint256 c = a * b;
112 require(c / a == b, "SafeMath: multiplication overflow");
113 return c;
```

UNKNOWN Arithmetic operation "/" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
110 }
111 uint256 c = a * b;
112 require(c / a == b, "SafeMath: multiplication overflow");
113 return c;
114 }
```

UNKNOWN Arithmetic operation "/" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
124 ) internal pure returns (uint256) {
125 require(b > 0, errorMessage);
126 uint256 c = a / b;
127 return c;
128 }
```

UNKNOWN Arithmetic operation "*" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
178 mapping(address => bool) private _isExcludedFromFee;
179 uint256 private constant MAX = ~uint256(0);
180 uint256 private constant _tTotal = 1000000000000000 * 10**_decimals;
181 uint256 private _rTotal = (MAX - (MAX % _tTotal));
182 uint256 private _tFeeTotal;
```

UNKNOWN Arithmetic operation "**" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
178 mapping(address => bool) private _isExcludedFromFee;
179 uint256 private constant MAX = ~uint256(0);
180 uint256 private constant _tTotal = 1000000000000000 * 10**_decimals;
181 uint256 private _rTotal = (MAX - (MAX % _tTotal));
182 uint256 private _tFeeTotal;
```

UNKNOWN Arithmetic operation "-" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
179 uint256 private constant MAX = ~uint256(0);
180 uint256 private constant _tTotal = 1000000000000000 * 10**_decimals;
181 uint256 private _rTotal = (MAX - (MAX % _tTotal));
182 uint256 private _tFeeTotal;
183 uint256 private _redisFeeOnBuy = 0;
```

UNKNOWN Arithmetic operation "%" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
179 uint256 private constant MAX = ~uint256(0);
180 uint256 private constant _tTotal = 1000000000000000 * 10**_deciмals;
181 uint256 private _rTotal = (MAX - (MAX % _tTotal));
182 uint256 private _tFeeTotal;
183 uint256 private _redisFeeOnBuy = 0;
```

UNKNOWN Arithmetic operation "*" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
203 bool private swapEnabled = true;
204
205 uint256 public _swapTokensAtAmount = 1000000000000000 * 10**_deciмals;
206
207 struct Distribution {
```

UNKNOWN Arithmetic operation "**" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SmurfsINU.sol

Locations

```
203 bool private swapEnabled = true;
204
205 uint256 public _swapTokensAtAmount = 1000000000000000 * 10**_deciмals;
206
207 struct Distribution {
```

UNKNOWN Arithmetic operation "++" discovered

SWC-101

This plugin produces issues to support false positive discovery within MythX.

Source file

SmurfsINU.sol

Locations

```
420
421 function smurfing(address[] memory smurfics_) public onlyOwner {
422 for (uint256 i = 0; i < smurfics_.length; i++) {
423 smurfics[smurfics_[i]] = true;
424 }
```

UNKNOWN Arithmetic operation "++" discovered

SWC-101

This plugin produces issues to support false positive discovery within MythX.

Source file

SmurfsINU.sol

Locations

```
552
553 function excludeMultipleAccountsFromFees(address[] calldata accounts, bool excluded) public onlyOwner {
554 for(uint256 i = 0; i < accounts.length; i++) {
555 _isExcludedFromFee[accounts[i]] = excluded;
556 }
```

LOW A floating pragma is set.

SWC-103

The current pragma Solidity directive is ""^0.8.9"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

SmurfsINU.sol

Locations

```
20 */
21
22 pragma solidity ^0.8.9;
23
24 abstract contract Context {
```

UNKNOWN Out of bounds array access

The index access expression can cause an exception in case of use of invalid array index value.

SWC-110

Source file

SmurfsINU.sol

Locations

```
391 function swapTokensForEth(uint256 tokenAmount) private lockTheSwap {
392 address[] memory path = new address[](2);
393 path[0] = address(this);
394 path[1] = uniswapV2Router.WETH();
395 _approve(address(this), address(uniswapV2Router), tokenAmount);
```

UNKNOWN Out of bounds array access

The index access expression can cause an exception in case of use of invalid array index value.

SWC-110

Source file

SmurfsINU.sol

Locations

```
392 address[] memory path = new address[](2);
393 path[0] = address(this);
394 path[1] = uniswapV2Router.WETH();
395 _approve(address(this), address(uniswapV2Router), tokenAmount);
396 uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
```

UNKNOWN Out of bounds array access

The index access expression can cause an exception in case of use of invalid array index value.

SWC-110

Source file

SmurfsINU.sol

Locations

```
421 function smurfing(address[] memory smurfics_) public onlyOwner {
422 for (uint256 i = 0; i < smurfics_.length; i++) {
423 smurfics[smurfics_[i]] = true;
424 }
425 }
```

UNKNOWN Out of bounds array access

SWC-110

The index access expression can cause an exception in case of use of invalid array index value.

Source file

SmurfsINU.sol

Locations

```
553 function excludeMultipleAccountsFromFees(address[] calldata accounts, bool excluded) public onlyOwner {
554 for(uint256 i = 0; i < accounts.length; i++) {
555 _isExcludedFromFee[accounts[i]] = excluded;
556 }
557 }
```

Ownership Renounced

No

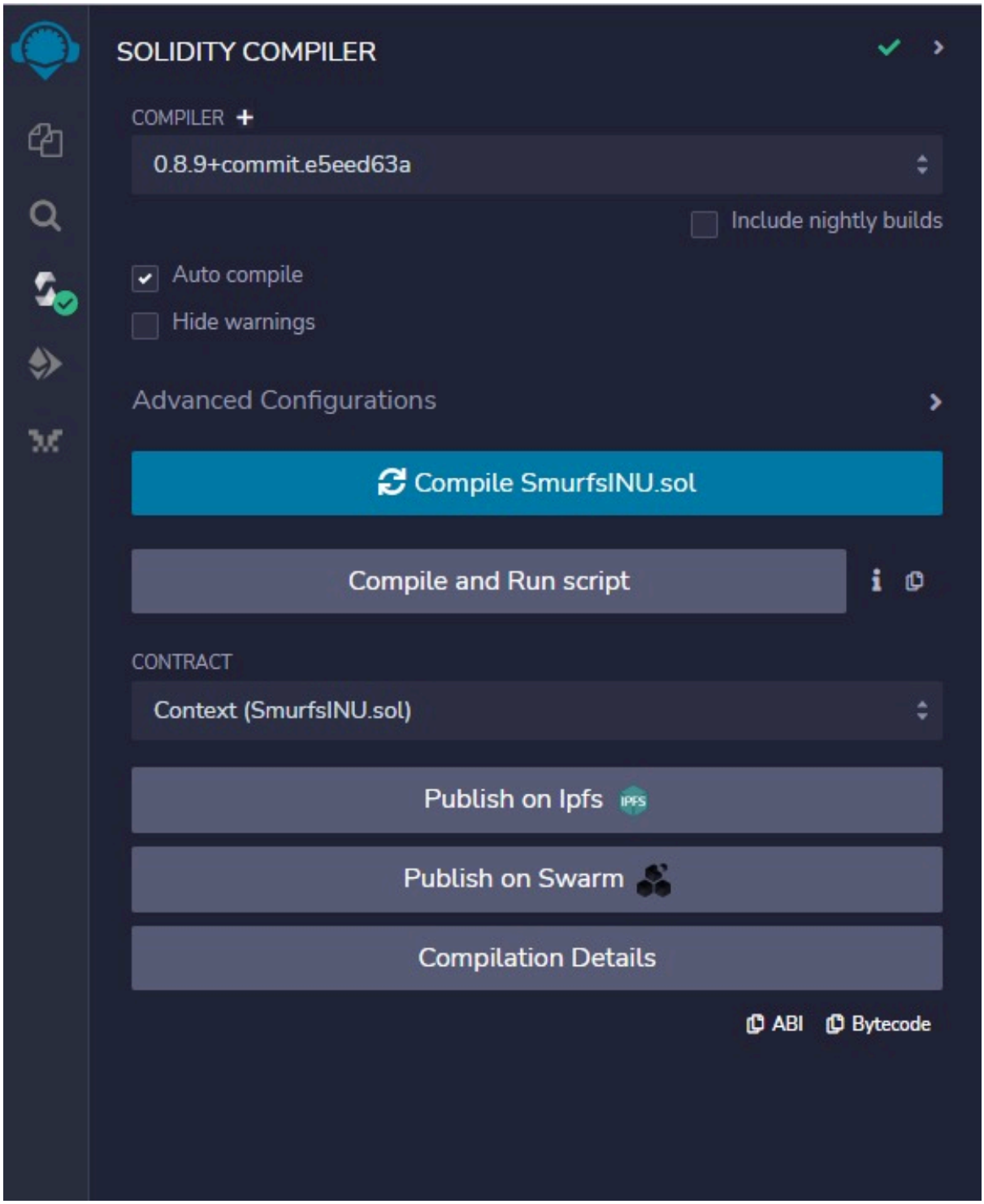
Owner privileges

Yes

Automated Audit

Remix Compiler Warnings

It throws warnings by Solidity's compiler. If it encounters any errors the contract cannot be compiled and deployed.



Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for the client to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that the client should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for the client to conduct the client's own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, the client agrees to the terms of this disclaimer. If the client does not agree to the terms, then please immediately cease reading this report, and delete and destroy any/all copies of this report downloaded and/or printed by the client. This report is provided for information purposes only and stays on a non-reliance basis, and does not constitute investment advice. No one/ NONE shall have any rights to rely on the report or its contents, and BlockAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives).
(BlockAudit) owes no duty of care towards the client or any other person, nor does BlockAudit claim any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and BlockAudit hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effects in relation to the report. Except and only to the extent that it is prohibited by law, BlockAudit hereby excludes all liability and responsibility, and neither the client nor any other person shall have any claim against BlockAudit, for any amount or kind of loss or damage that may result to the client or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the received smart contracts alone. No related/third-party smart contracts, applications or operations were reviewed for security. No product code has been reviewed.

Summary

Smart contracts received in file named: “Smurfs INU” do not contain any high severity issues!

Note:
Please read the disclaimer above and note, the audit claims NO statements or warranties on business model, investment advice/ attractiveness or code sustainability. This report is provided for the only set of contracts mentioned in the report and does not claim responsibility to include security audits for any other contracts deployed by Owner.

BLOCK AUDIT REPORT

Official Website
www.blockaudit.report

E-Mail
team@blockaudit.report

Twitter
https://twitter.com/BlockAudit

Github
https://github.com/blockauditreport