Smart Contract Security Audit

Audit details:

Audited project:	ONS
Deployer address	0xcaf8e42293973b767230c64663d2f4e22bbe873a
Blockchain:	Binance Smart Chain
Project website:	https://onsx.io

June, 2021
TechRate

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 you 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 you 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 you to conduct your 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, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make 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 TechRate 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 effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you 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 smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by ONS to perform an audit of smart contracts:

- *https://bscscan.com/address/0xcaf8e42293973b767230c64663d2f4e22bbe873a#code*

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

ONS Token contracts details

Token contract details for 20.06.2021.

Contract name:	ONS
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xcaf8e42293973b767230c64663d2f4e22bbe873a
Total supply:	1000000000000
Token ticker:	ONS
Decimals:	9
Token holders:	
Transactions count:	
Top 100 dominance:	100 %
Contract deployer address:	0xbcde3090054d4e99269c620572f2e98601485686
Contract's current owner address:	0xbcde3090054d4e99269c620572f2e98601485686

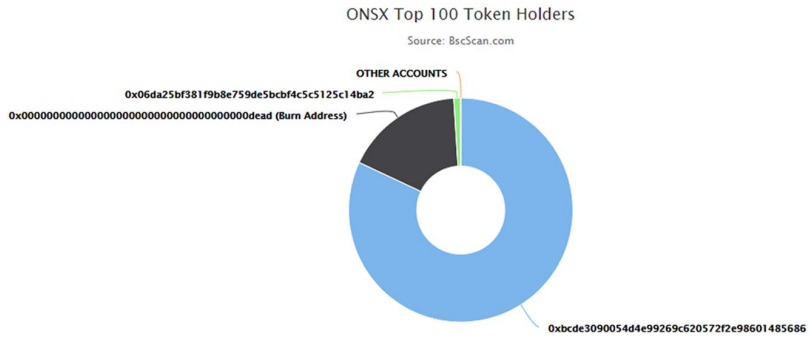
MasterChef contract details for 20.06.2021.

Contract name:	MasterChef
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0xcaf8e42293973b767230c64663d2f4e22bbe873a
Deployer address:	0xbcde3090054d4e99269c620572f2e98601485686
Dev address:	0xbcde3090054d4e99269c620572f2e98601485686
Burn address:	0x000000000000000000000000000000000000dead
ONS contract address:	0xcaf8e42293973b767230c64663d2f4e22bbe873a
ONS per block:	100000000000000000000
Contract owner address:	0xbcde3090054d4e99269c620572f2e98601485686
Pool length:	9
Start block:	6861909
Total alloc point:	7910
Bonus multiplier:	1

ONS token distribution

The top 100 holders collectively own 100.00% (1,000,000,000,000.00 Tokens) of ONSX

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 3



(A total of 1,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xbcde3090054d4e99269c620572f2e98601485686	820,000,000,000	82.0000%
2	Burn Address	170,000,000,000	17.0000%
3	0x06da25bf381f9b8e759de5bcbf4c5c5125c14ba2	10,000,000,000	1.0000%

ONS token top 3 token holders

(A total of 1,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xbcde3090054d4e99269c620572f2e98601485686	820,000,000,000	82.0000%
2	Burn Address	170,000,000,000	17.0000%
3	0x06da25bf381f9b8e759de5bcbf4c5c5125c14ba2	10,000,000,000	1.0000%

Issues Checking Status

№	Issue description.	Checking status
1	Compiler errors.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Low issues
10	Methods execution permissions.	Passed
11	Economy model of the contract.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Open Zeppelin contracts implementation and usage.	Passed
21	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Block gas limit

Issue:

The updateEmissionRate function can fail due to block gas limit if the pool size is too big.

Owner privileges

- Owner can change the burn address.
- Owner can change the lock day for withdrawals, this could be risky, if the owner will set the big number, then users will not be able to withdraw their funds for a long period of time.

  We recommend removing the lock time checking in emergency withdraw function, so users will be able to withdraw their funds without rewards any time they want!

- Owner can change the owner of the OctaX token through the MasterChef contract, but the owner of the OctaX token should be only the MasterChef contract.

Conclusion

Smart contracts contain low severity issues and owner privileges! Audited only the smart contracts listed above, LP-pair contracts and the other contracts of the project are not audited.

MasterChef contract differs from the GooseDefi fork and has time lock for withdrawals and emergency withdrawals, so users should be notified about the withdrawal time locks and check that carefully.

As mentioned above, we recommend removing the lock time checking in the emergency withdraw function!

Techrate note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.