Smart Contract Security Audit

Audit details:

Audited project: BNB30

Project Telegram:https://t.me/BNB30ChatTeam

Blockchain: BinanceSmartChain

Project website: https://bnb30.net

May 1, 2021

Audited By: Nick Patel

Smart Contract Security Auditor

SCAUDITS TELEGRAM: https://t.me/scauditor

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 SCAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SCAudit) owe no duty of care towards you or any other person, nor does SCAudit 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 SCAudit 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, SCAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SCAudit, 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

SCAudit was hired by BNB30.net to perform an audit of smart contracts:
https://bscscan.com/address/0x3c6279E231F81875c42143f232fBFd8e22E806B9

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

Withdraw functions looks clean. * Line 133/138: it is seen that if it is the first withdrawal it does not charge you the commission, for the next withdrawals it is seen that it charges 25% commission to leave in the bnb pool

```
115 ▾    function withdraw() public {
116          User storage user = users[msg.sender];
117
118          uint256 totalAmount = getUserDividends(msg.sender);
119
120          uint256 referralBonus = getUserReferralBonus(msg.sender);
121 ▾        if (referralBonus > 0) {
122              user.bonus = 0;
123              totalAmount = totalAmount.add(referralBonus);
124          }
125
126          require(totalAmount > 0, "User has no dividends");
127
128          uint256 contractBalance = address(this).balance;
129 ▾        if (contractBalance < totalAmount) {
130              totalAmount = contractBalance;
131          }
132
133 ▾        if(user.firstDeposit == 0){
134              user.firstDeposit = 1;
135 ▾        } else{
136              uint256 commission = totalAmount.mul(PROJECT_COMISSION).div(PERCENTS_DIVIDER);
137              totalAmount = totalAmount.sub(commission);
138          }
139
140          user.checkpoint = block.timestamp;
141
142          msg.sender.transfer(totalAmount);
143
144          emit Withdrawn(msg.sender, totalAmount);
145
146      }
```
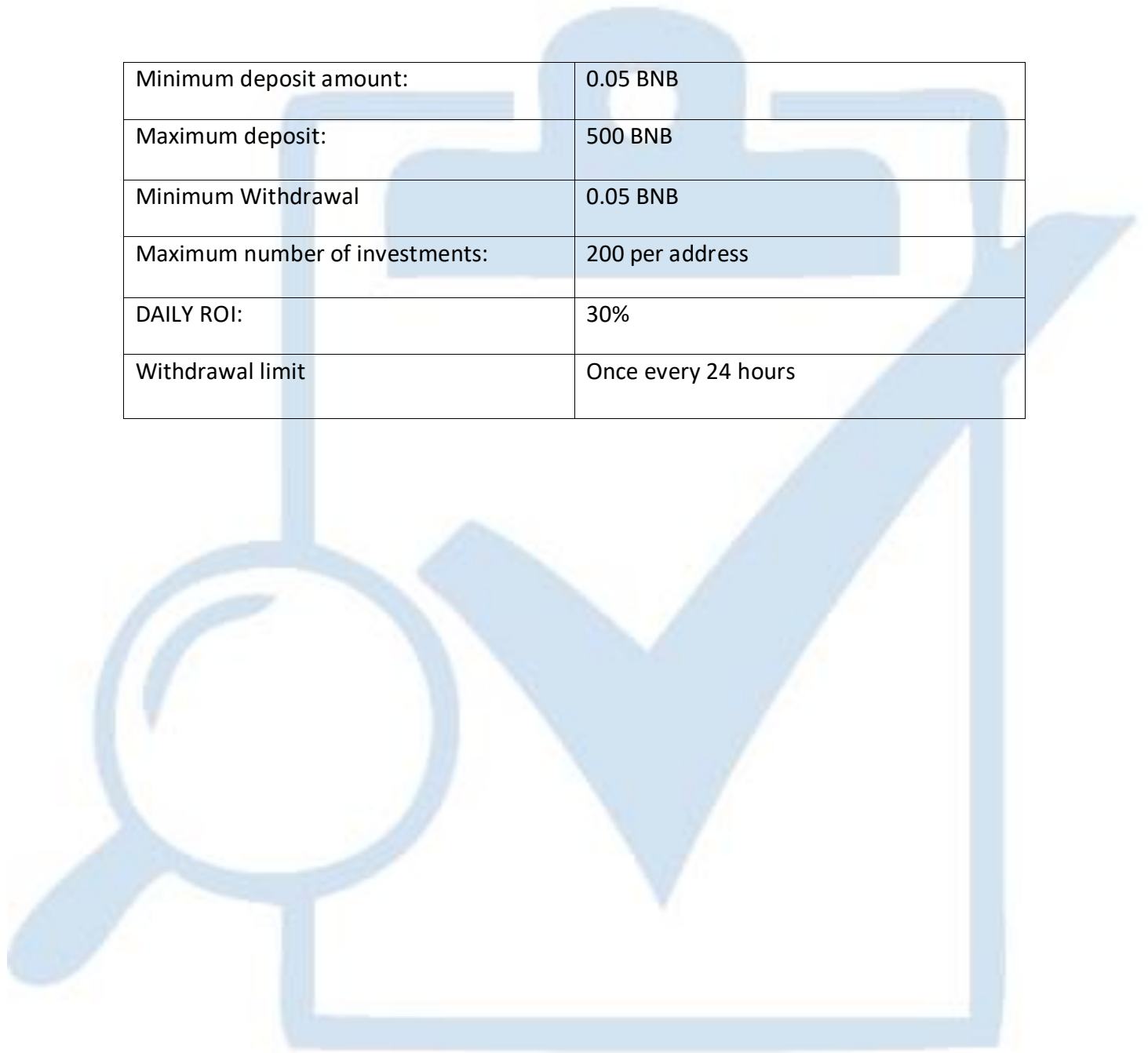
✓ By Auditing the contract of BNB30 we have found no vulnerabilities on the contract. No Backdoor Codes
✓ No Exit Scams
✓ No Faulty or Hidden Codes

ISSUES STATUS

№	Issue description	Checking status
1	Compiler warnings.	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.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	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 Zeppelin module.	Passed
21	Fallback function security.	Passed

CONTRACT DETAILS

Minimum deposit amount:	0.05 BNB
Maximum deposit:	500 BNB
Minimum Withdrawal	0.05 BNB
Maximum number of investments:	200 per address
DAILY ROI:	30%
Withdrawal limit	Once every 24 hours