Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

September, 2021

Audit Details

Audited project

ThaiRidgeBack

Deployer address

0x01024b042aba76751ed7d4ea9fcef3d534f61ebb

Client contacts:

ThaiRidgeBack team

Blockchain

Binance Smart Chain

Project website:

https://www.thairidgeback.space/

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 ThaiRidgeBack to perform an audit of smart contracts:

https://bscscan.com/address/0x7708343575e0e57168c4acd45a0f296939de7415#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.

Contracts Details

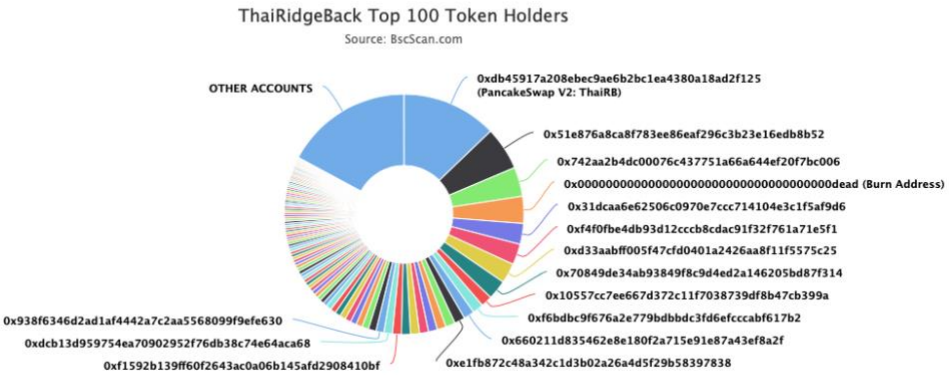
Token contract details for 07.09.2021

Contract name	ThaiRidgeBack
Contract address	0x7708343575E0e57168C4Acd45A0f296939DE7415
Total supply	10,000,000,000
Token ticker	ThaiRB
Decimals	4
Token holders	541
Transactions count	77,682
Top 100 holders dominance	82.86%
Contract deployer address	0x01024b042aba76751ed7d4ea9fcef3d534f61ebb
Contract's current owner address	0x0000000000000000000000000000000000000000

ThaiRidgeBack Token Distribution

The top 100 holders collectively own 82.86% (8,285,829,204.47 Tokens) of ThaiRidgeBack

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 541

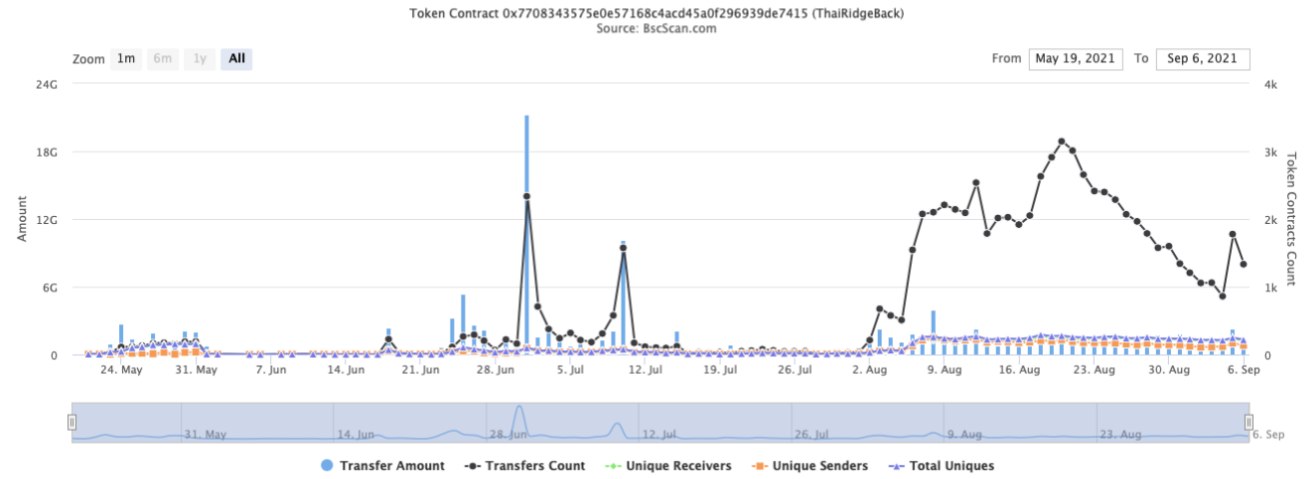


(A total of 8,285,829,204.47 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

ThaiRidgeBack Contract Interaction Details

Time Series: Token Contract Overview

Fri 21, May 2021 - Mon 6, Sept 2021



ThaiRidgeBack Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: ThaiRB	1,284,103,207.1629	12.8410%
2	0x51e876a8ca8f783ee86eaf296c3b23e16edb8b52	580,774,262.7501	5.8077%
3	0x742aa2b4dc00076c437751a66a644ef20f7bc006	394,888,889.2944	3.9489%
4	Burn Address	362,338,436.5836	3.6234%
5	0x31dcaa6e62506c0970e7ccc714104e3c1f5af9d6	280,879,432.1743	2.8088%
6	0xf4f0fbe4db93d12cccb8cdac91f32f761a71e5f1	279,121,323.8431	2.7912%
7	0xd33aabff005f47cfd0401a2426aa8f11f5575c25	271,775,851.333	2.7178%
8	0x70849de34ab93849f8c9d4ed2a146205bd87f314	262,620,490.8969	2.6262%
9	0x10557cc7ee667d372c11f7038739df8b47cb399a	150,045,027.4568	1.5005%
10	0xf6bdbc9f676a2e779bdbbdc3fd6efcccabf617b2	149,381,187.5173	1.4938%

Contract functions details

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Ext] maxSupply

+ Context
  - [Int] <Constructor> #
  - [Int] _msgSender
  - [Int] _msgData

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Int] _transferOwnership #

+ BEP20ThaiRB (Context, IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Ext] getOwner
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] totalSupply
  - [Ext] maxSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Pub] increaseAllowance #

- [Pub] decreaseAllowance #
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint #
- [Pub] burn #
  - modifiers: onlyOwner
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #

($) = payable function
= non-constant function

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.	Passed
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

No low severity issues found.

Owner privileges (In the period when the owner is not renounced)

- Owner can mint under _maxSupply.

```
function mint(address account, uint256 amount)
    public
    onlyOwner
    returns (bool)
{
    _mint(account, amount);
    return true;
}
```

- Owner can burn.

```
function burn(uint256 amount) public onlyOwner returns (bool) {
    _burn(_msgSender(), amount);
    return true;
}
```

Conclusion

Smart contracts do not contain high severity issues!

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.