



TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details



Audited project

Hermes



Deployer address

0xB8B8bD40A22A2cEfa307F40aA287189118978694



Client contacts:

Hermes team



Blockchain

Binance Smart Chain



Project website:

<https://luxolympus.finance>

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 Hermes to perform an audit of smart contracts:

<https://bscscan.com/address/0x6b9c32e4d0972d546cd63079b5fb3451fd73d251#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

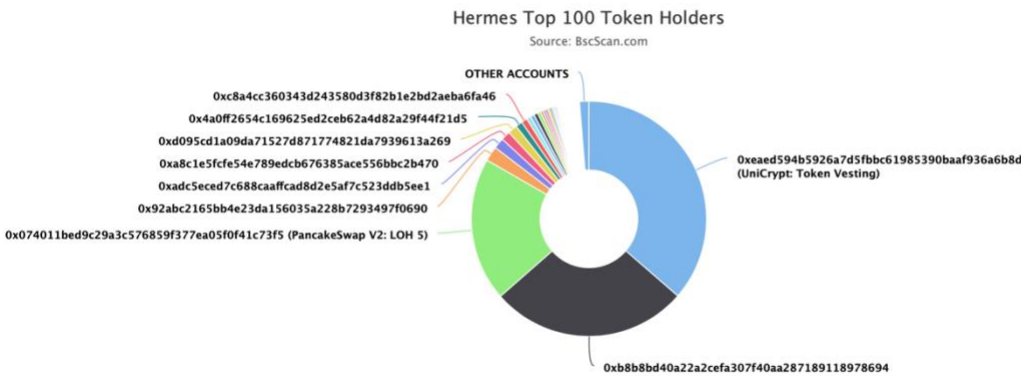
Token contract details for 26.11.2021

Contract name	Hermes
Contract address	0x6b9c32E4d0972D546Cd63079b5fb3451fd73d251
Total supply	110,000,000
Token ticker	LOH
Decimals	8
Token holders	209
Transactions count	921
Top 100 holders dominance	98.71%
Contract deployer address	0xB8B8bD40A22A2cEfa307F40aA287189118978694
Contract's current owner address	0xB8B8bD40A22A2cEfa307F40aA287189118978694

Hermes Token Distribution

The top 100 holders collectively own 98.71% (108,585,302.04 Tokens) of Hermes

Token Total Supply: 110,000,000.00 Token | Total Token Holders: 209

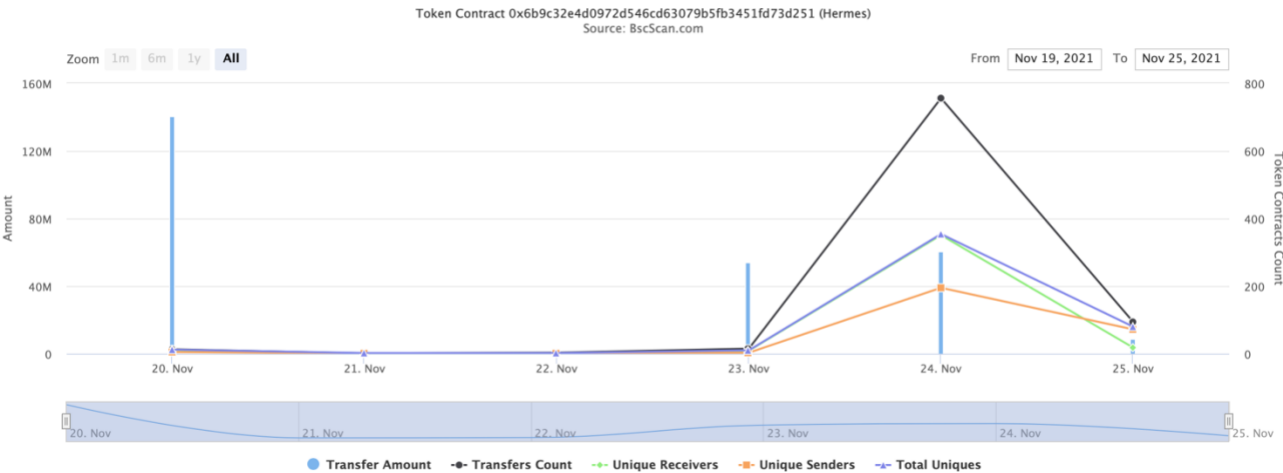


(A total of 108,585,302.04 tokens held by the top 100 accounts from the total supply of 110,000,000.00 token)


Hermes Contract Interaction Details

Time Series: Token Contract Overview

Sat 20, Nov 2021 - Thu 25, Nov 2021



Hermes Top 10 Token Holders

Rank	Address	Quantity	Percentage
1	 UniCrypt: Token Vesting	40,010,494.03263517	36.3732%
2	0xb8b8bd40a22a2cefa307f40aa287189118978694	29,912,380.46176997	27.1931%
3	PancakeSwap V2: LOH 5	21,715,465.97105787	19.7413%
4	0x92abc2165bb4e23da156035a228b7293497f0690	2,245,387.52672624	2.0413%
5	0xadc5eced7c688caaffcad8d2e5af7c523ddb5ee1	1,625,603.56380247	1.4778%
6	0xa8c1e5fcfe54e789edcb676385ace556bbc2b470	1,414,429.08865805	1.2858%
7	0xd095cd1a09da71527d871774821da7939613a269	1,409,413.14071094	1.2813%
8	0x4a0ff2654c169625ed2ceb62a4d82a29f44f21d5	1,025,976.11414096	0.9327%
9	0xc8a4cc360343d243580d3f82b1e2bd2aeba6fa46	900,312.65574518	0.8185%
10	0xcc41c1dab102a590e8c2dec4466cec6558aedf03	651,196.28903079	0.5920%



Contract functions details

- + [Int] IERC20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
- + [Int] IERC20Metadata (IERC20)
 - [Ext] name
 - [Ext] symbol
 - [Ext] decimals
- + Context
 - [Int] _msgSender
 - [Int] _msgData
- + Ownable (Context)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Int] _transferOwnership #
- + ERC20 (Context, IERC20, IERC20Metadata)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Int] _transfer #
 - [Int] _mint #
 - [Int] _burn #
 - [Int] _approve #
 - [Int] _beforeTokenTransfer #
 - [Int] _afterTokenTransfer #
- + HolderToken (ERC20, Ownable)
 - [Pub] <Constructor> (\$)
 - modifiers: ERC20
 - [Ext] <Fallback> (\$)
 - [Prv] getBalance

- [Pub] decimals
- [Pub] totalSupply
- [Pub] reflectionFee
- [Pub] isExcludedFromFee
- [Pub] balanceOf
- [Pub] isExcluded
- [Pub] totalFeesRedistributed
- [Pub] excludeFromFee #
 - modifiers: onlyOwner
- [Pub] includeInFee #
 - modifiers: onlyOwner
- [Pub] changeReflectionFee #
 - modifiers: onlyOwner
- [Prv] _mintStart #
- [Pub] reflect #
- [Pub] reflectionFromToken
- [Prv] tokenFromReflection
- [Pub] excludeAccountFromReward #
 - modifiers: onlyOwner
- [Pub] includeAccountInReward #
 - modifiers: onlyOwner
- [Int] _transfer #
- [Prv] _tokenTransfer #
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _getCompleteTaxValue
- [Prv] _getTransferValues
- [Prv] _reflectFee #
- [Prv] _getRate
- [Prv] _getCurrentSupply

(\$) = 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.	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. Out of gas

Issue:

- The function `includeAccountinReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function includeAccountinReward(address account) public onlyOwner() {
    require(!_isExcluded[account], "Account is already included");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function `_getCurrentSupply()` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;

    for(uint256 i = 0; i < _excluded.length; i++){
        if(_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) {
            return(_rTotal, _tTotal);
        }
        rSupply = rSupply - _rOwned[_excluded[i]];
        tSupply = tSupply - _tOwned[_excluded[i]];
    }

    if(rSupply < _rTotal / _tTotal) {
        return(_rTotal, _tTotal);
    }

    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

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

- Owner can include in and exclude from fees.

```
function excludeFromFee(address account) public onlyOwner() {
    _isExcludedFromFee[account] = true;
}

function includeInFee(address account) public onlyOwner() {
    _isExcludedFromFee[account] = false;
}
```

- Owner can change reflection fee.

```
function changeReflectionFee(uint256 newReflectionFee) public onlyOwner() returns(bool) {
    require(newReflectionFee >= 0, "Reflection fee must be greater or equal to zero");
    require(newReflectionFee <= 10, "Reflection fee must be lower or equal to ten");
    _reflectionFee = newReflectionFee;
    return true;
}
```

- Owner can include in and exclude from reward.

```
function excludeAccountFromReward(address account) public onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

function includeAccountInReward(address account) public onlyOwner() {
    require(_isExcluded[account], "Account is already included");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

Conclusion

Smart contracts contain low severity issues and owner privileges!
Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details are provided by the team:

<https://app.unicrypt.network/amm/pancake-v2/token/0x6b9c32E4d0972D546Cd63079b5fb3451fd73d251>

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.