QuillAudits

Audit Report
May, 2022

For

METAMERCE

Table of Content

Executive Summary

Project Name	MetaMerce
Overview	Metamerce is the first integrated city of amusement offering shopping, content creation or music composing, networking, professionally or on a friendly basis, chatting domains and 3D gaming.
Timeline	April 27, 2022 to May 4, 2022
Method	Manual Review, Functional Testing, Automated Testing etc.
Scope of Audit	The scope of this audit was to analyse Metamerce codebase for quality, security, and correctness.
Source Code	*https://github.com/metamerce/merce-token-BEP20/blob/main/metamerce.sol* *https://bscscan.com/address/0x618951276a25a7fed805c68c1813f1b8c39c7dd3#code*
Fixed In	*https://bscscan.com/address/0x6d163b653010740bfb41BED4bee23f94b3285cBA#code*

High
Medium
Low
Informational

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	1	4

Types of Severities

High

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

Checked Vulnerabilities

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- BEP20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Remix IDE, Truffle, Truffle Team, Solhint, Mythril, Slither, Solidity statistic analysis.

Manual Testing

A. Contract - Metamerce

High Severity Issues

No issues were found

Medium Severity Issues

No issues were found

Low Severity Issues

A.1 Missing address verification

Line 61, 67, 77, 84

```
ftrace | funcSig
function approve(address spender↑, uint tokens↑) public returns (bool success↑) {
    allowed[msg.sender][spender↑] = tokens↑;
    emit Approval(msg.sender, spender↑, tokens↑);
    return true;
}

ftrace | funcSig
function increaseApproval(address spender↑, uint tokens↑) public returns (bool success↑) {
    allowed[msg.sender][spender↑] = safeAdd(allowed[msg.sender][spender↑], tokens↑);
    return true;
}

ftrace | funcSig
function decreaseApproval(address spender↑, uint tokens↑) public returns (bool success↑) {
    allowed[msg.sender][spender↑] = safeSub(allowed[msg.sender][spender↑], tokens↑);
    return true;
}

ftrace | funcSig
function transfer(address to↑, uint tokens↑) public returns (bool success↑) {
    balances[msg.sender] = safeSub(balances[msg.sender], tokens↑);
    balances[to↑] = safeAdd(balances[to↑], tokens↑);
    emit Transfer(msg.sender, to↑, tokens↑);
    return true;
}

ftrace | funcSig
function transferFrom(address from↑, address to↑, uint tokens↑) public returns (bool success↑) {
    balances[from↑] = safeSub(balances[from↑], tokens↑);
    allowed[from↑][msg.sender] = safeSub(allowed[from↑][msg.sender], tokens↑);
    balances[to↑] = safeAdd(balances[to↑], tokens↑);
    emit Transfer(from↑, to↑, tokens↑);
    return true;
}
}
```

Description

Certain functions lack a safety check in the address, the address-type argument should include a zero-address test, otherwise, the contract's functionality may become inaccessible or tokens may be burned in perpetuity.

Remediation

It’s recommended to undertake further validation prior to user-supplied data. The concerns can be resolved by utilizing a whitelist technique or a modifier.

Status

Fixed

Informational Issues

A.2 Unlocked pragma (pragma solidity ^0.5.0)

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

Here all the in-scope contracts have an unlocked pragma, it is recommended to lock the same. Moreover, we strongly suggest not to use experimental Solidity features (e.g., pragma experimental ABIEncoderV2) or third-party unaudited libraries. If necessary, refactor the current code base to only use stable features.

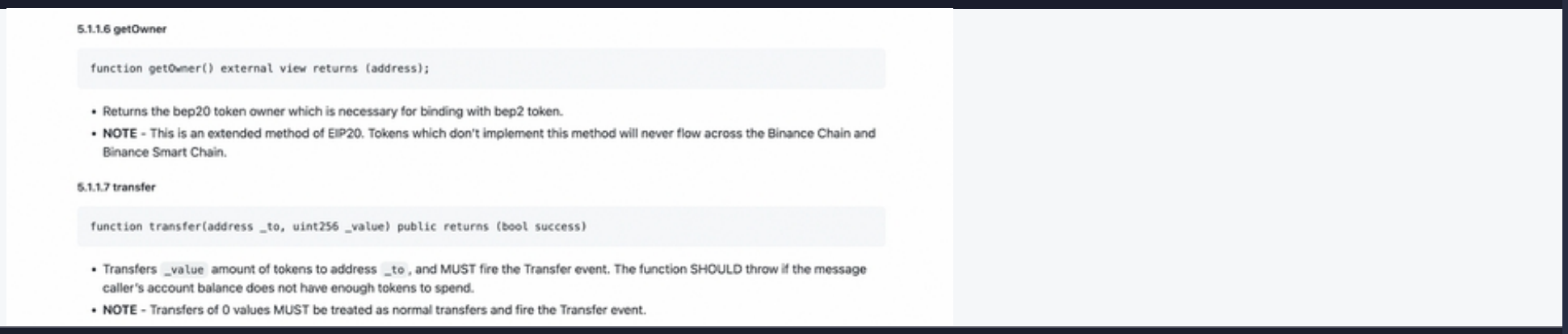
Status

Fixed

A.3 BEP20 Standard violation

Description

Implementation of transfer() function does not allow the input of zero amount as it's demanded in ERC20 and BEP20 standards. This issue may break the interaction with smart contracts that rely on full BEP20 support. Moreover, the GetOwner() function which is a mandatory function is missing from the contract.



5.1.1.6 getOwner

```
function getOwner() external view returns (address);
```

- Returns the bep20 token owner which is necessary for binding with bep2 token.
- **NOTE** - This is an extended method of EIP20. Tokens which don't implement this method will never flow across the Binance Chain and Binance Smart Chain.

5.1.1.7 transfer

```
function transfer(address _to, uint256 _value) public returns (bool success)
```

- Transfers `_value` amount of tokens to address `_to`, and MUST fire the Transfer event. The function SHOULD throw if the message caller's account balance does not have enough tokens to spend.
- **NOTE** - Transfers of 0 values MUST be treated as normal transfers and fire the Transfer event.

Remediation

The transfer function must treat zero amount transfer as a normal transfer and an event must be emitted. Moreover, it is recommended to implement getOwner() function.

Reference

https://github.com/bnb-chain/BEPs/blob/master/BEP20.md#5117-transfer

Status

Fixed

A.4 Missing Zero Check

Line 61, 67, 77, 84

```
ftrace | funcSig
61  function approve(address spender↑, uint tokens↑) public returns (bool success↑) {
62      allowed[msg.sender][spender↑] = tokens↑;
63      emit Approval(msg.sender, spender↑, tokens↑);
64      return true;
65  }
66
ftrace | funcSig
67  function increaseApproval(address spender↑, uint tokens↑) public returns (bool success↑) {
68      allowed[msg.sender][spender↑] = safeAdd(allowed[msg.sender][spender↑], tokens↑);
69      return true;
70  }
71
ftrace | funcSig
72  function decreaseApproval(address spender↑, uint tokens↑) public returns (bool success↑) {
73      allowed[msg.sender][spender↑] = safeSub(allowed[msg.sender][spender↑], tokens↑);
74      return true;
75  }
76
ftrace | funcSig
77  function transfer(address to↑, uint tokens↑) public returns (bool success↑) {
78      balances[msg.sender] = safeSub(balances[msg.sender], tokens↑);
79      balances[to↑] = safeAdd(balances[to↑], tokens↑);
80      emit Transfer(msg.sender, to↑, tokens↑);
81      return true;
82  }
83
ftrace | funcSig
84  function transferFrom(address from↑, address to↑, uint tokens↑) public returns (bool success↑) {
85      balances[from↑] = safeSub(balances[from↑], tokens↑);
86      allowed[from↑][msg.sender] = safeSub(allowed[from↑][msg.sender], tokens↑);
87      balances[to↑] = safeAdd(balances[to↑], tokens↑);
88      emit Transfer(from↑, to↑, tokens↑);
89      return true;
90  }
91  }
```

Description

Contracts lack zero address checks, hence are prone to be initialized with zero addresses.

Remediation

Consider adding zero address checks in order to avoid risks of incorrect contract initializations.

Status

Fixed

A.5 Public functions that could be declared external inorder to save gas

Description

Whenever a function is not called internally, it is recommended to define them as external instead of public in order to save gas. For all the public functions, the input parameters are copied to memory automatically, and it costs gas. If your function is only called externally, then you should explicitly mark it as external. External function's parameters are not copied into memory but are read from calldata directly. This small optimization in your solidity code can save you a lot of gas when the function input parameters are huge.

Here is a list of function that could be declared external:

- totalSupply()
- name()
- symbol()
- decimals()
- increaseAllowance()
- decreaseAllowance()

Status

Fixed

Functional Testing

Some of the tests performed are mentioned below

- Should be able call all getters
- Should be able to transfer token
- Should be able to approve
- Should be able to increaseApprove
- Should be able to decreaseApprove
- Should be able to transferFrom
- Should revert if transfer amount exceeds balance

Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

Closing Summary

In this report, we have considered the security of the Metamerce. We performed our audit according to the procedure described above.

Some issues of Low and informational severity were found, Some suggestions and best practices are also provided in order to improve the code quality and security posture.

At the End, Metamerce Team Resolved all Issues

Disclaimer

QuillAudits smart contract audit is not a security warranty, investment advice, or an endorsement of the Metamerce Platform. This audit does not provide a security or correctness guarantee of the audited smart contracts.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the Metamerce Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

500+
Audits Completed

$15B
Secured

500K
Lines of Code Audited

Follow Our Journey

Audit Report
May, 2022

For

METAMERCE

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com