InterFi NETWORK

SMART CONTRACT AUDIT

interfinetwork

hello@interfi.network

https://interfi.network

PREPARED FOR

VENOM STAKING AND REWARDER

INTRODUCTION

Auditing Firm	InterFi Network
Client Firm	Venom
Methodology	Automated Analysis, Manual Code Review
Language	Solidity
Staking Contract	0x6bdF40ad11F526A2de9Fe5f2928d41a1C1D8DF93
Rewarder Contract	0xAd45fE74bBeB7d7Eb36F98f44085D8a53Ef1aEac
Blockchain	Ethereum Chain
Centralization	Active ownership via Gnosis Safe
Commit	34ac8f265cec4e637c181957040db14da7aaa219
Website	http://venomcrypto.io/
Telegram	https://t.me/VenomERC/
Twitter	https://twitter.com/VenomCryptoVNM/
Prelim Report Date	January 22, 2023
StakingV2 Report Date	May 20, 2023

ℹ️ Verify the authenticity of this report on our website: https://www.interfi.network/audits

EXECUTIVE SUMMARY

InterFi has performed the automated and manual analysis of solidity codes. Solidity codes were reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical 🔴	Major 🟠	Medium 🟡	Minor 🟢	Informational 🔵
Open	0	0	0	1	2
Acknowledged	0	0	1	1	0
Resolved	0	1	2	0	1
Noteworthy Privileges	Refer to PAGE 20 for centralization related privileges				

ℹ️ Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

ℹ️ Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.

TABLE OF CONTENTS

SCOPE OF WORK

InterFi was consulted by Venom to conduct the smart contract audit of their solidity source codes. The audit scope of work is strictly limited to mentioned solidity file(s) only:

- VenomStaking.sol
- VenomRewarder.sol

ℹ️ If source codes are not deployed on the main net, they can be modified or altered before main-net deployment. Verify the contract's deployment status below:

Public Contract Link	
https://etherscan.io/address/0x6bdF40ad11F526A2de9Fe5f2928d41a1C1D8DF93#code	
Contract Name	VenomStaking
Compiler Version	0.8.17
License	MIT

Public Contract Link	
https://etherscan.io/address/0xAd45fE74bBeB7d7Eb36F98f44085D8a53Ef1aEac#code	
Contract Name	VenomRewarder
Compiler Version	0.8.17
License	MIT

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of InterFi's auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
  - Remix IDE Developer Tool
  - Open Zeppelin Code Analyzer
  - SWC Vulnerabilities Registry
  - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges. We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	○ Token Supply Manipulation ○ Access Control and Authorization ○ Assets Manipulation ○ Ownership Control ○ Liquidity Access ○ Stop and Pause Trading ○ Ownable Library Verification

Common Contract Vulnerabilities	○ Integer Overflow ○ Lack of Arbitrary limits ○ Incorrect Inheritance Order ○ Typographical Errors ○ Requirement Violation ○ Gas Optimization ○ Coding Style Violations ○ Re-entrancy ○ Third-Party Dependencies ○ Potential Sandwich Attacks ○ Irrelevant Codes ○ Divide before multiply ○ Conformance to Solidity Naming Guides ○ Compiler Specific Warnings ○ Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to solidity codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH

- The client may use the audit report internally or disclose it publicly.

ℹ️ It is important to note that there is no pass or fail in the audit, it is recommended to view the audit as an unbiased assessment of the safety of solidity codes.

RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical 🔴	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major 🟠	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium 🟡	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor 🟢	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Informational ⚫	These risks pose little severity to the contract or those who interact with it. They should be highlighted nonetheless.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- Privileged roles can be granted the power to `pause()` the contract in case of an external attack.
- Privileged roles can use functions like, `include()`, and `exclude()` to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- The client can lower centralization-related risks by implementing below mentioned practices:
- Privileged role's private key must be carefully secured to avoid any potential hack.
- Privileged role should be shared by multi-signature (multi-sig) wallets.
- Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.
- Renouncing the contract ownership, and privileged roles.
- Remove functions with elevated centralization risk.

ℹ Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.

AUTOMATED ANALYSIS

Symbol	Definition
🛑	Function modifies state
💸	Function is payable
🔒	Function is internal
🔐	Function is private
!	Function is important

Venom Staking

ReentrancyGuard	Implementation			
└	<Constructor>	Public !	🛑	NO!
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public !	🛑	NO!
└	owner	Public !		NO!
└	renounceOwnership	Public !	🛑	onlyOwner
└	transferOwnership	Public !	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑	
Pausable	Implementation	Context		
└	<Constructor>	Public !	🛑	NO!
└	paused	Public !		NO!
└	_pause	Internal 🔒	🛑	whenNotPaused
└	_unpause	Internal 🔒	🛑	whenPaused

IERC20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	<Constructor>	Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
└	totalSupply	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	transfer	Public ❗	🛑	NO❗
└	allowance	Public ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_spendAllowance	Internal 🔒	🛑	

└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
Address	Library			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionStaticCall	Internal 🔒		
└	functionStaticCall	Internal 🔒		
└	functionDelegateCall	Internal 🔒	🛑	
└	functionDelegateCall	Internal 🔒	🛑	
└	verifyCallResult	Internal 🔒		
SafeERC20	Library			
└	safeTransfer	Internal 🔒	🛑	
└	safeTransferFrom	Internal 🔒	🛑	
└	safeApprove	Internal 🔒	🛑	
└	safeIncreaseAllowance	Internal 🔒	🛑	
└	safeDecreaseAllowance	Internal 🔒	🛑	
└	_callOptionalReturn	Private 🔐	🛑	
SafeMath	Library			
└	tryAdd	Internal 🔒		
└	trySub	Internal 🔒		
└	tryMul	Internal 🔒		
└	tryDiv	Internal 🔒		
└	tryMod	Internal 🔒		
└	add	Internal 🔒		
└	sub	Internal 🔒		

└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	sub	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
Math	Library			
└	max	Internal 🔒		
└	min	Internal 🔒		
└	average	Internal 🔒		
└	ceilDiv	Internal 🔒		
EnumerableSet	Library			
└	_add	Private 🔐	🛑	
└	_remove	Private 🔐	🛑	
└	_contains	Private 🔐		
└	_length	Private 🔐		
└	_at	Private 🔐		
└	_values	Private 🔐		
└	add	Internal 🔒	🛑	
└	remove	Internal 🔒	🛑	
└	contains	Internal 🔒		
└	length	Internal 🔒		
└	at	Internal 🔒		
└	values	Internal 🔒		
└	add	Internal 🔒	🛑	
└	remove	Internal 🔒	🛑	
└	contains	Internal 🔒		
└	length	Internal 🔒		
└	at	Internal 🔒		

└	values	Internal 🔒		
└	add	Internal 🔒	🛑	
└	remove	Internal 🔒	🛑	
└	contains	Internal 🔒		
└	length	Internal 🔒		
└	at	Internal 🔒		
└	values	Internal 🔒		
IVenom	Interface			
└	updateRewardsMultiplier	External !	🛑	NO!
IVenomRewarder	Interface			
└	transferRewards	External !	🛑	NO!
VenomStaking	Implementation	Ownable, Pausable, ReentrancyGuard		
└	<Constructor>	Public !	🛑	NO!
└	setEndTime	External !	🛑	onlyOwner
└	restartPeriod	External !	🛑	onlyOwner
└	setRewardCycle	External !	🛑	onlyOwner
└	deposit	External !	🛑	nonReentrant whenNotPaused updateReward updateUserList
└	withdraw	Public !	🛑	nonReentrant updateReward updateUserList
└	UpdateRewardsMultiplier	External !	🛑	onlyOwner
└	withdrawAll	External !	🛑	NO!
└	claim	Public !	🛑	nonReentrant updateReward updateUserList
└	claimable	External !		NO!
└	_safeTransferDividends	Internal 🔒	🛑	
└	setRewardRate	External !	🛑	onlyOwner
└	setPenaltyFee	External !	🛑	onlyOwner
└	setFeeRecipient	External !	🛑	onlyOwner
└	_removeUser	Internal 🔒	🛑	
└	_checkOrAddUser	Internal 🔒	🛑	
└	userCount	External !		NO!

| └ | userList | External ❗ | | onlyOwner |

| └ | pause | External ❗ | 🛑 | onlyOwner |

| └ | unpause | External ❗ | 🛑 | onlyOwner |

Venom Rewarder

| **ReentrancyGuard** | Implementation | |||

| └ | <Constructor> | Public ❗ | 🛑 | NO❗ |

||||||

| **Context** | Implementation | |||

| └ | _msgSender | Internal 🔒 | | |

| └ | _msgData | Internal 🔒 | | |

||||||

| **Ownable** | Implementation | Context |||

| └ | <Constructor> | Public ❗ | 🛑 | NO❗ |

| └ | owner | Public ❗ | | NO❗ |

| └ | _checkOwner | Internal 🔒 | | |

| └ | renounceOwnership | Public ❗ | 🛑 | onlyOwner |

| └ | transferOwnership | Public ❗ | 🛑 | onlyOwner |

| └ | _transferOwnership | Internal 🔒 | 🛑 | |

||||||

| **IAccessControl** | Interface | |||

| └ | hasRole | External ❗ | | NO❗ |

| └ | getRoleAdmin | External ❗ | | NO❗ |

| └ | grantRole | External ❗ | 🛑 | NO❗ |

| └ | revokeRole | External ❗ | 🛑 | NO❗ |

| └ | renounceRole | External ❗ | 🛑 | NO❗ |

||||||

| **Strings** | Library | |||

| └ | toString | Internal 🔒 | | |

| └ | toHexString | Internal 🔒 | | |

| └ | toHexString | Internal 🔒 | | |

| └ | toHexString | Internal 🔒 | | |

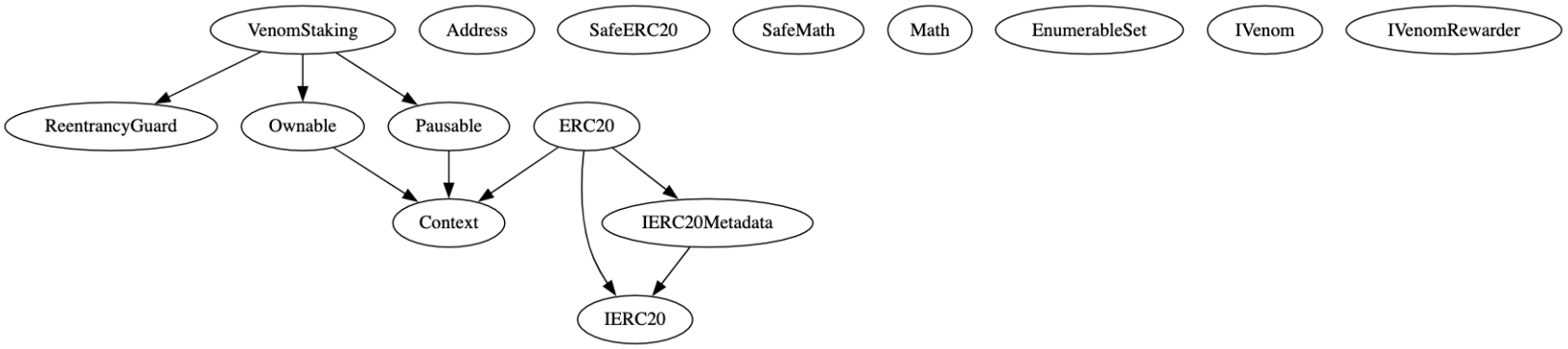
IERC165	Interface			
└	supportsInterface	External ❗		NO❗
ERC165	Implementation	IERC165		
└	supportsInterface	Public ❗		NO❗
AccessControl	Implementation	Context, IAccessControl, ERC165		
└	supportsInterface	Public ❗		NO❗
└	hasRole	Public ❗		NO❗
└	_checkRole	Internal 🔒		
└	_checkRole	Internal 🔒		
└	getRoleAdmin	Public ❗		NO❗
└	grantRole	Public ❗	🛑	onlyRole
└	revokeRole	Public ❗	🛑	onlyRole
└	renounceRole	Public ❗	🛑	NO❗
└	_setupRole	Internal 🔒	🛑	
└	_setRoleAdmin	Internal 🔒	🛑	
└	_grantRole	Internal 🔒	🛑	
└	_revokeRole	Internal 🔒	🛑	
IERC20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗

└	decimals	External ❗		NO❗
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	<Constructor>	Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
└	totalSupply	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	transfer	Public ❗	🛑	NO❗
└	allowance	Public ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_spendAllowance	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
Address	Library			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionStaticCall	Internal 🔒		

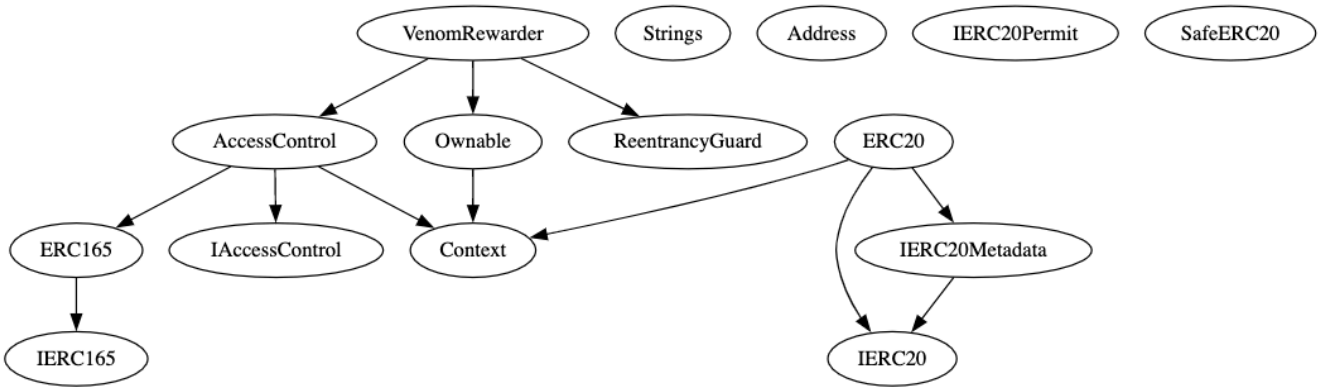
```
| └ | functionStaticCall | Internal 🔒 |   | |
| └ | functionDelegateCall | Internal 🔒 | 🛑  | |
| └ | functionDelegateCall | Internal 🔒 | 🛑  | |
| └ | verifyCallResult | Internal 🔒 |   | |
||||||
| **IERC20Permit** | Interface |  |||
| └ | permit | External ❗️ | 🛑  |NO❗️ |
| └ | nonces | External ❗️ |   |NO❗️ |
| └ | DOMAIN_SEPARATOR | External ❗️ |   |NO❗️ |
||||||
| **SafeERC20** | Library |  |||
| └ | safeTransfer | Internal 🔒 | 🛑  | |
| └ | safeTransferFrom | Internal 🔒 | 🛑  | |
| └ | safeApprove | Internal 🔒 | 🛑  | |
| └ | safeIncreaseAllowance | Internal 🔒 | 🛑  | |
| └ | safeDecreaseAllowance | Internal 🔒 | 🛑  | |
| └ | safePermit | Internal 🔒 | 🛑  | |
| └ | _callOptionalReturn | Private 🔐 | 🛑  | |
||||||
| **VenomRewarder** | Implementation | Ownable, ReentrancyGuard, AccessControl |||
| └ | <Constructor> | Public ❗️ | 🛑  |NO❗️ |
| └ | transferRewards | External ❗️ | 🛑  | nonReentrant onlyPool |
| └ | withdrawToken | External ❗️ | 🛑  | onlyOwner |
| └ | setPool | External ❗️ | 🛑  | onlyOwner |
```

INHERITANCE GRAPH

Venom Staking



Venom Rewarder



MANUAL REVIEW

Identifier	Definition	Severity
CEN-01	Centralization privileges of Venom Staking and Rewarder	Major 🟠

Important centralized privileges are listed below:

Venom Staking

`setEndTime()`
`restartPeriod()`
`setRewardCycle()`
`UpdateRewardsMultiplier()`
`setRewardRate()`
`setPenaltyFee()`
`setFeeRecipient()`
`userList()`
`pause()`
`unpause()`

Venom Rewarder

`transferRewards()`
`withdrawToken()`
`setPool()`

RECOMMENDATION

Deployer and/or contract owner private keys must be secured carefully. Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

RESOLUTION

Venom team has appointed Gnosis multi-sig wallet 0x4d03Ff6f4d19E9b3578E2708b8811ca6D2F32531 as owner for both staking and rewarder contracts.

Identifier	Definition	Severity
CEN-05	Privileged role performing pause contract in Venom Staking	Medium 🟡

In Venom Staking, privileged role can call `pause()`

```
function pause() external onlyOwner {
    _pause();
}

function unpause() external onlyOwner {
    _unpause();
}
```


RECOMMENDATION

Remove pause, as it can intentionally stop smart contract function modules.

RESOLUTION

Venom team has implemented pause for `deposit()` only which is activated when staking pool is ended.

Identifier	Definition	Severity
LOG-01	Improper of arbitrary limits	Minor

Below mentioned functions are set with high or no arbitrary limits.

```
UpdateRewardsMultiplier()
setPenaltyFee()
```


RECOMMENDATION

These functions should be provided arbitrary limits, e.g., put a `require` check that allows maximum penalty fee change up to 20%.

ACKNOWLEDGEMENT

Venom team has introduced maximum fee limit; however, the maximum fee can be set up to 50%.

Identifier	Definition	Severity
LOG-02	Re-entrancy	Medium 🟡

Below mentioned functions are used without re-entrancy guard:

`_safeTransferDividends()` – `call` function can be used by malicious contract's fallback function, it can call back to the staking contract, re-entering the `_safeTransferDividends()` function before the transfer completes. Specified `gas: 3000` may limit recursive calls, however this method to protect against re-entrancy is not full-proof.

Note: `claim()` function with the `nonReentrant` modifier is protected against re-entrancy, but `_safeTransferDividends` itself is not.

RECOMMENDATION

Use Checks Effects Interactions pattern when handing over the flow to an external entity and/or guard functions against re-entrancy attacks. Re-entrancy guard is used to prevent re-entrant calls. Learn more: https://consensys.github.io/smart-contract-best-practices/attacks/reentrancy/

RESOLUTION

Venom team has iterated that `_safeTransferDividends()` is only used by `claim()`.

Identifier	Definition	Severity
LOG-03	Inadequate access control and visibility check	Medium 🟡

In Venom Staking, below mentioned functions are used with inadequate access control and visibility check:

```
withdrawAll()
claimable()
updateRewardsMultiplier()
transferRewards()
```


RECOMMENDATION

Access control interactions, interface calls, external and public calls must be authenticated adequately to avoid possible vulnerabilities.

ACKNOWLEDGEMENT

Venom project team has acknowledged to keep aforementioned functions `external`. Contract logic requires these functions to be accessible.

Identifier	Definition	Severity
VNM-01	Hardcoded Venom contract address	Minor

Venom contract address 0x804ea14b08dEc488e5B0bC408f23EEf107fE3717 is hardcoded in Venom Staking contract.

RECOMMENDATION

Provide a function to change venom contract address if needed in the future.

Identifier	Definition	Severity
COD-04	Improper error messages	Informational

In Venom Rewarder, below mentioned `require` statements should be provided accurate information string:

Lines 1776, 1799, 1830

In Venom Rewarder, below mentioned `require` statements should be provided accurate information string:

Lines 1529, 1540, 1548

RECOMMENDATION

Provide accurate information strings for `require` related errors.

RESOLUTION

Error messages are fixed in the deployed version.

Identifier	Definition	Severity
COD-08	Lack of fallback function	Informational

Fallback functions are usually executed in one of the following cases: If a function identifier doesn't match any of the available functions in a smart contract. If there was no data supplied along with the function call.

RECOMMENDATION

Use fallback function with empty data, and mark it external, and payable.

Identifier	Definition	Severity
COD-10	Third Party Dependencies	Informational

Smart contract is interacting with third party protocols e.g., Market Makers, Open Zeppelin. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect third party dependencies regularly, and mitigate severe impacts whenever necessary.

DISCLAIMERS

InterFi Network provides the easy-to-understand audit of solidity source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way

to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, INTERFI NETWORK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. InterFi Network does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.

LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than InterFi Network. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites' and social accounts' owners. You agree that InterFi Network is not responsible for the content or operation of such websites and social accounts and that InterFi Network shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

ABOUT INTERFI NETWORK

InterFi Network provides intelligent blockchain solutions. We provide solidity development, testing, and auditing services. We have developed 150+ solidity codes, audited 1000+ smart contracts, and analyzed 500,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Velas, Oasis, etc.

InterFi Network is built by engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 4 core members, and 6+ casual contributors.

Website: https://interfi.network

Email: hello@interfi.network

GitHub: https://github.com/interfinetwork

Telegram (Engineering): https://t.me/interfiaudits

Telegram (Onboarding): https://t.me/interfisupport

interfinetwork

hello@interfi.network

https://interfi.network

SMART CONTRACT AUDITS | SOLIDITY DEVELOPMENT AND TESTING

RELENTLESSLY SECURING PUBLIC AND PRIVATE BLOCKCHAINS