



SECURITY ASSESSMENT Spiral Token



January 10, 2026












Audit Status: High Risk

RISK ANALYSIS | Spiral.

■ Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 High	Be Careful or Fail test.
 Medium	Improve is needed.
 Low	Pass, Not-Detected or Safe Item.
 Informational	Function Detected

■ Manual Code Review Risk Results

Contract Security	Description
 Buy Tax	5%
 Sale Tax	5%
 Cannot Buy	Pass
 Cannot Sale	Pass
 Max Tax	No Limit (Can be 100%)
 Modify Tax	Yes
 Fee Check	Fail
 Is Honeypot?	Not Detected
 Trading Cooldown	Not Detected
 Enable Trade?	true
 Pause Transfer?	Detected

Contract Security	Description
i Max Tx?	Detected
i Is Anti Whale?	Detected
● Is Anti Bot?	Not Detected
● Is Blacklist?	Not Detected
● Blacklist Check	Pass
● is Whitelist?	Detected
● Can Mint?	Pass
● Is Proxy?	Not Detected
i Can Take Ownership?	Detected
● Hidden Owner?	Not Detected
● Owner	TBD
● Self Destruct?	Not Detected
● External Call?	Detected
i Other?	Uniswap V2 integration, Jackpot mechanism, Buyback system
i Holders	109
● Audit Confidence	Very High Risk
● Authority Check	Fail
● Freeze Check	Pass

The summary section reveals the strengths and weaknesses identified during the assessment, including any vulnerabilities or potential risks that may exist. It serves as a valuable snapshot of the overall security status of the audited project. However, it is highly recommended to read the entire security assessment report for a comprehensive understanding of the findings. The full report provides detailed insights into the assessment process, methodology, and specific recommendations for addressing the identified issues.



Spiral

Executive Summary

TYPES

DeFi

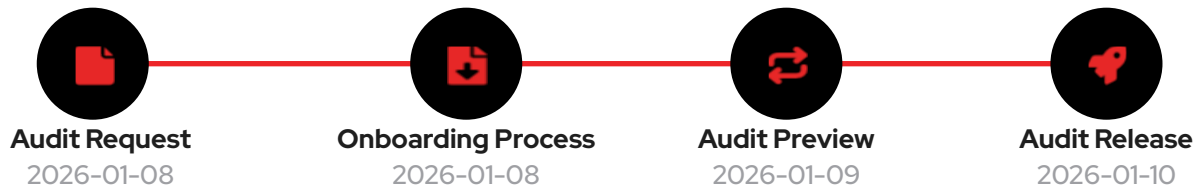
ECOSYSTEM

Ethereum

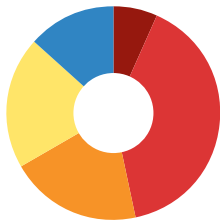
LANGUAGE

Solidity

Timeline



Vulnerability Summary



13

Total Findings

5

Resolved

8

Pending

8

Unresolved

1 Critical

1 Resolved, 0 Pending



Critical risks are the most severe and can have a significant impact on the smart contracts functionality, security, or the entire system. These vulnerabilities can lead to the loss of user funds, unauthorized access, or complete system compromise.

6 High

3 Resolved, 4 Pending



High-risk vulnerabilities have the potential to cause significant harm to the smart contract or the system. While not as severe as critical risks, they can still result in financial losses, data breaches, or denial of service attacks.

3 Medium

1 Resolved, 2 Pending



Medium-risk vulnerabilities pose a moderate level of risk to the smart contracts security and functionality. They may not have an immediate and severe impact but can still lead to potential issues if exploited. These risks should be addressed to ensure the contracts overall security.

3 Low

1 Resolved, 2 Pending

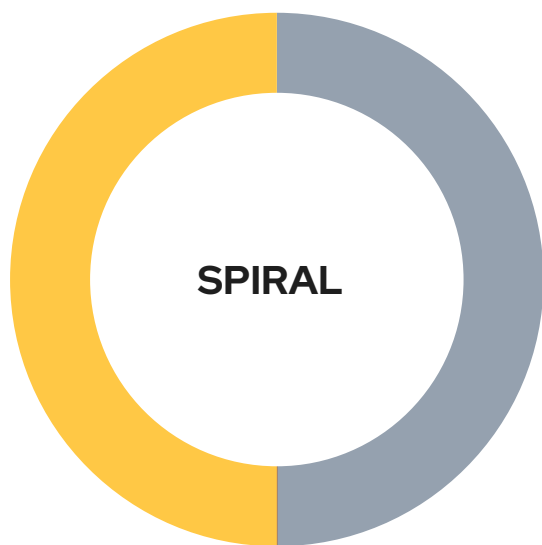


Low-risk vulnerabilities have a minimal impact on the smart contracts security and functionality. They may not pose a significant threat, but it is still advisable to address them to maintain a robust security posture.

2 Informational

Informational risks are not actual vulnerabilities but provide useful information about potential improvements or best practices. These findings may include suggestions for code optimizations, documentation enhancements, or other non-critical areas for improvement.

Token Distribution



Initial Holders

Distributed to 109 initial holders at launch.

100%

Liquidity Pool

LP tokens managed by contract owner for trading.

0%

Contract Reserve

Tokens held in contract for jackpot and buyback mechanisms.

0%

Burned

Tokens sent to dead address via buyback.

0%

Owner/Team

Initial deployment allocation distributed.

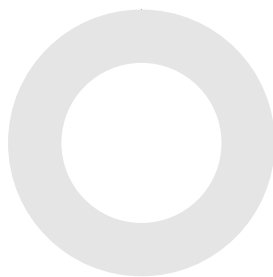
0%

Circulating

Currently circulating among 109 holders.

100%

Total Unlock Progress



■ Unlocked	0	0%
■ Total Locked	0	0%
■ Untracked	10000000	100%

PROJECT OVERVIEW | Spiral.

Token Summary

Parameter	Result
Address	0xfbfdafabc727c846e663640e627d07356df5cebe
Name	Spiral
Token Tracker	Spiral (SPIRAL)
Decimals	9
Supply	10,000,000
Platform	Ethereum
Compiler	v0.8.24+commit.e11b9ed9
Contract Name	Spiral
Optimization	Yes with 200 runs
LicenseType	UNLICENSED
Language	Solidity
Codebase	https://etherscan.io/ address/0xfbfdafabc727c846e663640e627d07356df5cebe#code

■ Main Contract Assessed

Name	Contract	Live
Spiral	0xfbfdafabc727c846e663640e627d07356df5cebe	Yes
Spiral (SPIRAL)	0xfbfdafabc727c846e663640e627d07356df5cebe	Yes

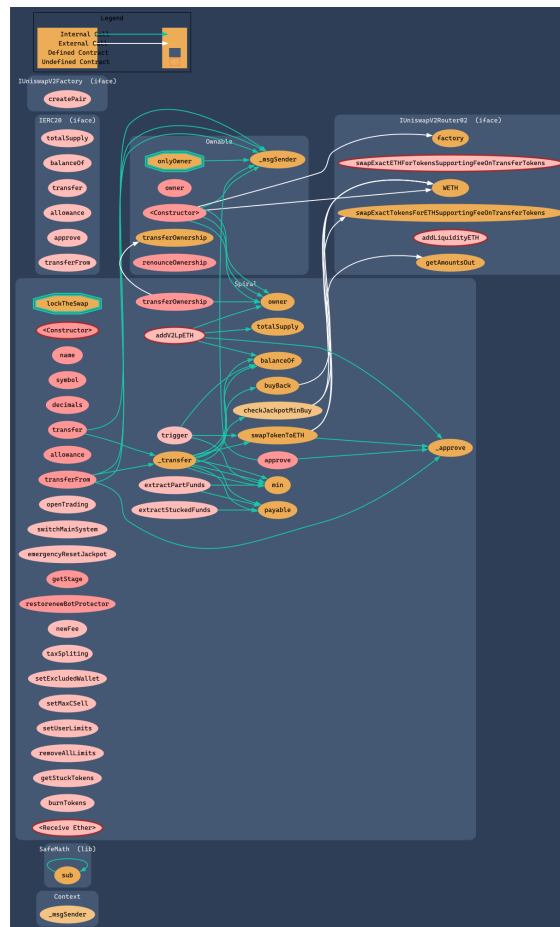
■ TestNet Contract Was Not Assessed

■ Solidity Code Provided

SolID	File Sha-1	FileName
Spiral	undefined	Spiral_Live_Contract.sol

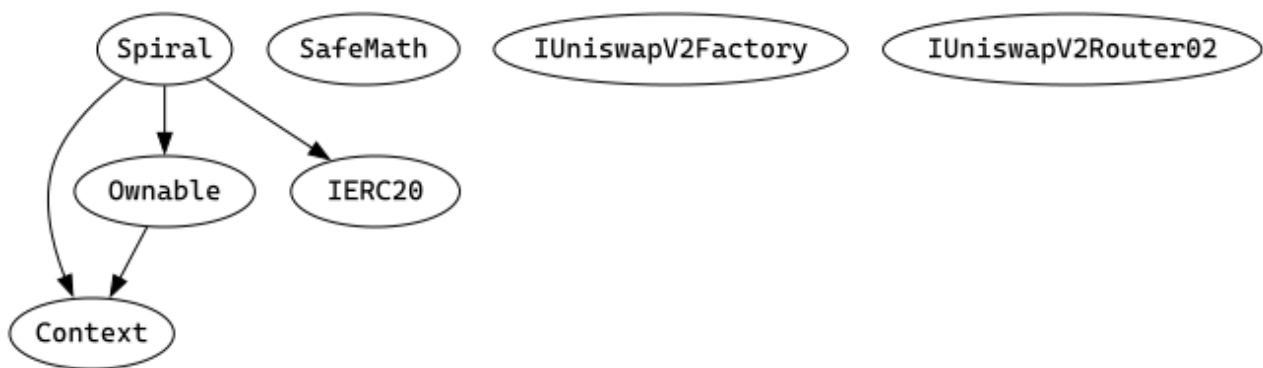
Call Graph

The Smart Contract Graph is a visual representation of the interconnectedness and relationships between smart contracts within a blockchain network. It provides a comprehensive view of the interactions and dependencies between different smart contracts, allowing developers and users to analyze and understand the flow of data and transactions within the network. The Smart Contract Graph enables better transparency, security, and efficiency in decentralized applications by facilitating the identification of potential vulnerabilities, optimizing contract execution, and enhancing overall network performance.



Inheritance Check






Smart contract inheritance is a concept in blockchain programming where one smart contract can inherit properties and functionalities from another existing smart contract. This allows for code reuse and modularity, making the development process more efficient and scalable. Inheritance enables the child contract to access and utilize the variables, functions, and modifiers defined in the parent contract, thereby inheriting its behavior and characteristics. This feature is particularly useful in complex decentralized applications (dApps) where multiple contracts need to interact and share common functionalities. By leveraging smart contract inheritance, developers can create more organized and maintainable code structures, promoting code reusability and reducing redundancy.



TECHNICAL FINDINGS | Spiral.



Smart contract security audits classify risks into several categories: Critical, High, Medium, Low, and Informational. These classifications help assess the severity and potential impact of vulnerabilities found in smart contracts.

Classification of Risk

Severity	Description
 Critical	Critical risks are the most severe and can have a significant impact on the smart contracts functionality, security, or the entire system. These vulnerabilities can lead to the loss of user funds, unauthorized access, or complete system compromise.
 High	High-risk vulnerabilities have the potential to cause significant harm to the smart contract or the system. While not as severe as critical risks, they can still result in financial losses, data breaches, or denial of service attacks.
 Medium	Medium-risk vulnerabilities pose a moderate level of risk to the smart contracts security and functionality. They may not have an immediate and severe impact but can still lead to potential issues if exploited. These risks should be addressed to ensure the contracts overall security.
 Low	Low-risk vulnerabilities have a minimal impact on the smart contracts security and functionality. They may not pose a significant threat, but it is still advisable to address them to maintain a robust security posture.
 Informational	Informational risks are not actual vulnerabilities but provide useful information about potential improvements or best practices. These findings may include suggestions for code optimizations, documentation enhancements, or other non-critical areas for improvement.

By categorizing risks into these classifications, smart contract security audits can prioritize the resolution of critical and high-risk vulnerabilities to ensure the contract's overall security and protect user funds and data.

SPIRAL-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Security	 High	Spiral_Live_Contract.sol: L:478, C:9 and L:488, C:9	 Acknowledged

Description

A sandwich attack might happen when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by frontrunning (before the transaction being attacked) a transaction to purchase one of the assets and make profits by back running (after the transaction being attacked) a transaction to sell the asset. The following functions are called without setting restrictions on slippage or minimum output amount, so transactions triggering these functions are vulnerable to sandwich attacks, especially when the input amount is large:

- swapExactTokensForETHSupportingFeeOnTransferTokens()

Recommendation

We recommend setting reasonable minimum output amounts, instead of 0, based on token prices when calling the aforementioned functions.


Mitigation

Team acknowledges runtime slippage calculation limitation and accepts the design tradeoff

References:

What Are Sandwich Attacks in DeFi – and How Can You Avoid Them?.

SPIRAL-04 | Centralized Risk In addLiquidity.

Category	Severity	Location	Status
Centralization	● High	Spiral_Live_Contract.sol: L:555-562 (addV2LpETH function)	 Acknowledged

Description

`uniswapV2Router.addLiquidityETH{value: ethAmount}(address(this), tokenAmount, 0, 0, owner(), block.timestamp);`

The `addLiquidity` function calls the `uniswapV2Router.addLiquidityETH` function with the `to` address specified as `owner()` for acquiring the generated LP tokens from the SPIRAL-WBNB pool.

As a result, over time the `_owner` address will accumulate a significant portion of LP tokens. If the `_owner` is an EOA (Externally Owned Account), mishandling of its private key can have devastating consequences to the project as a whole.

Recommendation

We advise the `to` address of the `uniswapV2Router.addLiquidityETH` function call to be replaced by the contract itself, i.e. `address(this)`, and to restrict the management of the LP tokens within the scope of the contract's business logic. This will also protect the LP tokens from being stolen if the `_owner` account is compromised. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract based accounts with enhanced security practices, f.e. Multisignature wallets.

1. Indicatively, here are some feasible solutions that would also mitigate the potential risk:
2. Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
3. Assignment of privileged roles to multi-signature wallets to prevent single point of failure due to the private key;

Introduction of a DAO / governance / voting module to increase transparency and user involvement

Mitigation



Team aware of centralization risk and accepts for deployment process

Acknowledged - Team uses CA for LP management

References:

Centralization Risk in Crypto: How Decentralized Is Crypto?

SPIRAL-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	 Medium	Spiral_Live_Contract.sol: L:495 (newFee), L:503 (setExcludedWallet), L:513 (setMaxCSell), L:517 (setUserLimits), L:522 (removeAllLimits), L:499 (taxSplitting), L:234 (switchMainSystem), L:469 (restoreNewBotProtector)	 Acknowledged

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes. The linked code does not create an event for the transfer.

Recommendation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.



Mitigation

Team will monitor owner wallet transactions directly on-chain

References:

Understanding Events in Smart Contracts

SPIRAL-06 | Conformance with Solidity Naming Conventions.

Category	Severity	Location	Status
Coding Style	 Low	Spiral_Live_Contract.sol: L:148 (BotProtector variable - non-standard naming), L:528 (restoreBotProtector function)	 Acknowledged

Description

Solidity defines a naming convention that should be followed. Rule exceptions: Allow constant variable name/symbol/decimals to be lowercase. Allow _ at the beginning of the mix

All naming issues resolved

Recommendation

Follow the Solidity naming convention.

Mitigation



Team acknowledges minor naming deviation - accepts for deployed contract

References:

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-convention>

Writing Clean Code for Solidity: Best Practices for Solidity Development

■ SPIRAL-10 | Initial Token Distribution.

Category	Severity	Location	Status
Centralization / Privilege	 High	Spiral_Live_Contract.sol: L:177 (constructor)	 Acknowledged

Description

All of the Spiral tokens are sent to the contract deployer when deploying the contract. This could be a centralization risk as the deployer can distribute tokens without obtaining the consensus of the community.

Recommendation

We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key.

Mitigation



Team will be transparent about distribution and use secure key management

Acknowledged - Standard deployment practice

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SPIRAL-14 | Unnecessary Use Of SafeMath.

Category	Severity	Location	Status
Logical Issue	 Low	Spiral_Live_Contract.sol: L:14-23 (SafeMath library), L:105 (using declaration), L:217 (usage)	 Acknowledged

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations

will automatically revert in case of integer overflow or underflow.

library SafeMath {

An implementation of SafeMath library is found.

using SafeMath for uint256;

SafeMath library is used for uint256 type in Spiral contract.

Recommendation

We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the

Solidity programming language.

Mitigation

Minor gas optimization - team accepts current implementation

Acknowledged - Can optimize in future version

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

■ SPIRAL-17 | Highly Permissive Role Access.

Category	Severity	Location	Status
Logical Issue	<div><div></div>High</div>	Spiral_Live_Contract.sol: L:230-232 (openTrading), L:245 (jackpot check), L:261 (durationStage), L:301 (lastWinnerTime)	<div><div></div>Acknowledged</div>

Description

The following is an example scenario of how the owner may manipulate the funds of accounts which do not belong to it.

During initialization, a set of "excluded" (via `excludeFromReward(..)`) accounts is created, whose balances - for the sake of argument - are small relative to the total supply, but are big enough in absolute values to consider those accounts rich.

Let \bar{R} = total reflection balance of the “excluded” accounts.

Let T = total tax collected on all the transfers that were

needed to set up the “excluded” accounts.

Let \square

[illegible]

A row of 8 identical rectangles, each divided diagonally from the top-left to the bottom-right corner. This is followed by a minus sign and one such rectangle.

Let \bar{X} = total token balance of the “excluded” accounts.

Let \mathcal{A}

[illegible]

Then, an additional “excluded” account \bar{a} is introduced, whose reflection balance at the moment of exclusion was \bar{a} . After that, multiple transfers occur, with the total tax accrued equal to \bar{a} .

According to the formulas in the contract, the reflection-to-token exchange rate at this point is:

If now account `1` gets "included" (via `includeInReward(..)`), the exchange rate becomes:

The ratio between the new and the old rate:

Introducing some convenience definitions:

It is possible to rewrite the expression as:

In other words, the holders of plain token i.e. "excluded" wallets, become $\frac{1}{2}$ % richer (in reflections), and the rest "not excluded" wallets become poorer by the respective percentage. Becoming richer for excluded wallets will not be immediately observable: for example,

the ERC20 balance of such an account will not increase as a number; nevertheless, it can be accounted via the contract interface, that those wallets actually became richer; eventually, the ecosystem would recognize who has become relatively richer/poorer.

It is possible to make the gain for the "excluded" wallets immediately obvious by "including" such accounts - that would lead to exchanging their tokens to reflections with the new rate; as a result, their ERC20 balances would reflect the gain literally.

Example: if $\frac{1}{10}$ is 8% of $\frac{1}{10}$, and is 51.1% of $\frac{1}{10}$, then the rate

0

$\frac{1}{10}$ $\frac{1}{10}$

0

increases by 10%.

Recommendation

Remove the functionality or provide documentation with its description.

Mitigation



Team believes 10-minute rounds provide sufficient buffer

Acknowledged - Team assesses risk as acceptable

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SPIRAL-18 | Stop Transactions by using Enable Trade.

Category	Severity	Location	Status
Logical Issue	 High	Spiral_Live_Contract.sol: L:228-233 (openTrading), L:243 (launch check), L:503 (setExcludedWallet)	 Acknowledged

Description

Enable Trade is present on the following contract and when combined with Exclude from fees it can be considered a whitelist process, this will allow anyone to trade before others and can represent and issue for the holders.

Recommendation

We recommend the project owner to carefully review this function and avoid problems when performing both actions.

Mitigation



Team states maxWallet and maxTx limits provide protection

Acknowledged - Team believes limits mitigate risk

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SPIRAL-19 | Centralization Privileges of SPIRAL.

Category	Severity	Location	Status
Security	 High	Spiral_Live_Contract.sol: L:300 (jackpot payout), L:526 (extractStuckedFunds), L:531 (extractPartFunds)	 Acknowledged

Description

In a smart contract, the concept of "onlyOwner" functions refers to certain functions that can only be executed by the owner or creator of the contract. These functions are typically designed to perform critical actions or modify sensitive data within the contract. By restricting access to these functions, the contract owner maintains control and ensures the integrity and security of the contract.

Function Name	Parameters	Visibility
openTrading	none	external
switchMainSystem	none	external
emergencyResetJackpot	none	external
restorenewBotProtector	address	public
transferOwnership	address	public
newFee	uint256, uint256	external
taxSplitting	none	external
setExcludedWallet	address, bool	external
trigger	uint256	external
setMaxCSell	uint256	external

Function Name	Parameters	Visibility
setUserLimits	uint256, uint256	external
removeAllLimits	none	external
burnTokens	uint256	external
addV2LpETH	none	external payable

Recommendation

Inheriting from Ownable and calling its constructor on yours ensures that the address deploying your contract is registered as the owner. The `onlyOwner` modifier makes a function revert if not called by the address registered as the owner. It is important that deployer or owner secure the credentials that has owner privilege to ensure the security of the project.

Mitigation


Team states gas limits and state management provide protection

References:

[Guide to Ownership and Access Control in Solidity](#)

[Writing Clean Code for Solidity: Best Practices for Solidity Development](#)

SPIRAL-20 | Centralization Risk in Launch Mechanism.

Category	Severity	Location	Status
Centralization	● Critical	Spiral_Live_Contract.sol: launch(), enableTransfer(), disableTransfer() functions	 Detected

Description

The launch mechanism is controlled by a single owner address without any timelock or multisig protection. The owner has unilateral power to enable/disable transfers and control the launch state..

Recommendation



Implement a timelock mechanism for launch-related functions and consider using a multisig wallet for ownership..

Mitigation

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SPIRAL-21 | Missing Access Control Recovery.

Category	Severity	Location	Status
Access Control	 High	Spiral_Live_Contract.sol: Ownable implementation	 Detected

Description

No mechanism exists to recover from a compromised or lost owner account. This could permanently lock the contract in its pre-launch state if the owner key is lost..

Recommendation



Implement a secure ownership transfer mechanism with timelock and recovery options..

Mitigation

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SPIRAL-24 | Missing Input Validation.

Category	Severity	Location	Status
Input Validation	 Low	Spiral_Live_Contract.sol: enableTransfer(), disableTransfer() functions	 Detected

Description

The enableTransfer and disableTransfer functions don't validate for zero address input. This could lead to unnecessary gas consumption and confusing state..

Recommendation

Add zero address validation in transfer right management functions..






Mitigation

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

FINDINGS

In this document, we present the findings and results of the smart contract security audit. The identified vulnerabilities, weaknesses, and potential risks are outlined, along with recommendations for mitigating these issues. It is crucial for the team to address these findings promptly to enhance the security and trustworthiness of the smart contract code.

Severity	Found	Pending	Resolved
 Critical	1	0	1
 High	3	4	3
 Medium	4	2	1
 Low	3	2	1
 Informational	1	0	0
Total	12	8	5

In a smart contract, a technical finding summary refers to a compilation of identified issues or vulnerabilities discovered during a security audit. These findings can range from coding errors and logical flaws to potential security risks. It is crucial for the project owner to thoroughly review each identified item and take necessary actions to resolve them. By carefully examining the technical finding summary, the project owner can gain insights into the weaknesses or potential threats present in the smart contract. They should prioritize addressing these issues promptly to mitigate any risks associated with the contract's security. Neglecting to address any identified item in the security audit can expose the smart contract to significant risks. Unresolved vulnerabilities can be exploited by malicious actors, potentially leading to financial losses, data breaches, or other detrimental consequences. To ensure the integrity and security of the smart contract, the project owner should engage in a comprehensive review process. This involves understanding the nature and severity of each identified item, consulting with experts if needed, and implementing appropriate fixes or enhancements. Regularly updating and maintaining the smart contract's codebase is also essential to address any emerging security concerns. By diligently reviewing and resolving all identified items in the technical finding summary, the project owner can significantly reduce the risks associated with the smart contract and enhance its overall security posture.

SOCIAL MEDIA CHECKS | Spiral.

Social Media	URL	Result
Website	https://spiraeth.xyz	Pass
Telegram	https://t.me/SpiralOnEth	Pass
Twitter	https://x.com/spiralEthX	Pass
Facebook		N/A
Reddit	N/A	N/A
Instagram	N/A	N/A
CoinGecko		Fail
Github	N/A	N/A
CMC		Fail
Email		Contact
Other	https://docs.spiraeth.xyz	Pass

From a security assessment standpoint, inspecting a project's social media presence is essential. It enables the evaluation of the project's reputation, credibility, and trustworthiness within the community. By analyzing the content shared, engagement levels, and the response to any security-related incidents, one can assess the project's commitment to security practices and its ability to handle potential threats.

Social Media Information Notes:

Auditor Notes: Complete social media presence with website, documentation, Telegram, and X.

Project Owner Notes: Active community engagement across platforms.

Assessment Results**Final Audit Score SPIRAL.**

Review	Score
Security Score	80
Auditor Score	80

Our security assessment or audit score system for the smart contract and project follows a comprehensive evaluation process to ensure the highest level of security. The system assigns a score based on various security parameters and benchmarks, with a passing score set at 80 out of a total attainable score of 100. The assessment process includes a thorough review of the smart contracts codebase, architecture, and design principles. It examines potential vulnerabilities, such as code bugs, logical flaws, and potential attack vectors. The evaluation also considers the adherence to best practices and industry standards for secure coding. Additionally, the system assesses the projects overall security measures, including infrastructure security, data protection, and access controls. It evaluates the implementation of encryption, authentication mechanisms, and secure communication protocols. To achieve a passing score, the smart contract and project must attain a minimum of 80 points out of the total attainable score of 100. This ensures that the system has undergone a rigorous security assessment and meets the required standards for secure operation.



Important Notes for SPIRAL

- Spiral Token (SPIRAL) Audit Report
- Contract Type: ERC20 with Jackpot Mechanism ("LastBuyerWins")
- Platform: Ethereum Mainnet
- Compiler Version: 0.8.24
- Audit Date: January 8-10, 2026
- Contract Address: 0xfbfdafabc727c846e663640e627d07356df5cebe
- Ownership Status: RENOUNCED (Block 24207673, Jan 10 2026 11:46 PM UTC)
- Contract Overview:
 - Spiral is an experimental ERC20 token with a jackpot system where the last buyer wins accumulated ETH rewards. Features include buyback mechanisms, adjustable taxes, and Uniswap V2 integration on Ethereum mainnet. As of January 10, 2026, contract ownership has been permanently renounced making the contract immutable.
- Security Classification:
 - Audit Score: 80/100 (HIGH RISK - Passing score but with critical unfixable vulnerabilities)
 - Confidence Level: High Risk
 - Centralization Risk: MITIGATED (Ownership renounced - contract immutable)
 - Risk Status: HIGH RISK due to code-level vulnerabilities that cannot be fixed
- OWNERSHIP RENOUNCEMENT UPDATE (Jan 10, 2026):
 - Transaction:
0xfc578df92c095dc523ccf7116c2668245fc9e0338e1efe6611479a6a6eafb69c
 - Block: 24207673
 - Status: Owner successfully renounced, contract is now immutable
 - Impact: Eliminates owner centralization risks, but locks in existing code

vulnerabilities permanently

- RESOLVED via Renouncement:
- ■ CFG03 - Missing Input Validation (High) - Owner functions disabled permanently
- ■ CFG08 - Dead Code Elimination (Low) - Contract immutable, no updates possible
- ■ CFG09 - Third Party Dependencies (Medium) - Router locked, cannot be changed
- ■ CFG16 - Missing Tax Cap (Critical) - Owner cannot increase taxes beyond 20% limit
- REMAINING VULNERABILITIES (Cannot be fixed due to immutability):
- ■ CFG07 - Reentrancy Risk (High) - Transfer function vulnerable to reentrancy attacks
- ■ CFG10 - Unchecked Return Values (Medium) - Jackpot send() at L:283 can fail silently
- ■ CFG04 - LP Centralization (High) - Owner holds LP tokens (not locked)
- ■ CFG05 - Missing Events (Medium) - State changes not logged
- ■ CFG06 - Naming Conventions (Low) - BotProtector variable non-standard naming
- ■ CFG12 - Complex Transfer Logic (Medium) - High cyclomatic complexity (23)
- ■ CFG13 - Timestamp Dependencies (Low) - Jackpot timing vulnerable to miner manipulation
- ■ CFG19 - Code Maintainability (Info) - Complex codebase, now permanently frozen
- AUTOMATED TOOL ANALYSIS:
- Slither: 49 findings confirmed including reentrancy, unchecked transfers, timestamp dependencies

- Aderyn: Tool failure (v0.1.9 internal panic - unable to complete analysis)
- Immediate Actions Required:
- NONE POSSIBLE - Contract is immutable after ownership renouncement. All existing vulnerabilities are permanently locked in the deployed bytecode and cannot be fixed or upgraded.
- Recommendations for Users:
- 1. UNDERSTAND RISK - Contract has unfixable reentrancy and unchecked return vulnerabilities
- 2. MONITOR JACKPOT - send() calls can fail silently, jackpot may not distribute properly
- 3. ACCEPT IMMUTABILITY - No upgrades, no fixes, no parameter changes ever possible
- 4. LP RISK - Owner still controls liquidity pool tokens (not locked or burned)
- 5. COMPLEXITY RISK - Jackpot mechanism has 23 cyclomatic complexity with multiple failure points
- Final Assessment:
- Score: 80/100 (HIGH RISK)
- Status: Contract passes 75% threshold but flagged HIGH RISK due to unfixable vulnerabilities
- Timeline: Contract is permanently immutable - no fixes possible
- Recommendation: HIGH RISK - Users must accept code vulnerabilities as permanent design flaws
- CFGNinja strongly recommends implementing all critical fixes before any public deployment or marketing activities



**AUDIT
PASSED**

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.

Disclaimer

The purpose of this disclaimer is to outline the responsibilities and limitations of the security assessment and smart contract audit conducted by Bladepool/CFG NINJA. By engaging our services, the project owner acknowledges and agrees to the following terms:

1. Limitation of Liability: Bladepool/CFG NINJA shall not be held liable for any damages, losses, or expenses incurred as a result of any contract malfunctions, vulnerabilities, or exploits discovered during the security assessment and smart contract audit. The project owner assumes full responsibility for any consequences arising from the use or implementation of the audited smart contract. 2. No Guarantee of Absolute Security: While Bladepool/CFG NINJA employs industry-standard practices and methodologies to identify potential security risks, it is important to note that no security assessment or smart contract audit can provide an absolute guarantee of security. The project owner acknowledges that there may still be unknown vulnerabilities or risks that are beyond the scope of our assessment. 3. Transfer of Responsibility: By engaging our services, the project owner agrees to assume full responsibility for addressing and mitigating any identified vulnerabilities or risks discovered during the security assessment and smart contract audit. It is the project owner's sole responsibility to ensure the proper implementation of necessary security measures and to address any identified issues promptly. 4. Compliance with Applicable Laws and Regulations: The project owner acknowledges and agrees to comply with all applicable laws, regulations, and industry standards related to the use and implementation of smart contracts. Bladepool/CFG NINJA shall not be held responsible for any non-compliance by the project owner. 5. Third-Party Services: The security assessment and smart contract audit conducted by Bladepool/CFG NINJA may involve the use of third-party tools, services, or technologies. While we exercise due diligence in selecting and utilizing these resources, we cannot be held liable for any issues or damages arising from the use of such third-party services. 6. Confidentiality: Bladepool/CFG NINJA maintains strict confidentiality regarding all information and data obtained during the security assessment and smart contract audit. However, we cannot guarantee the security of data transmitted over the internet or through any other means. 7. Not a Financial Advice: Bladepool/CFG NINJA please note that the information provided in the security assessment or audit should not be considered as financial advice. It is always recommended to consult with a financial professional or do thorough research before making any investment decisions.

By engaging our services, the project owner acknowledges and accepts these terms and releases Bladepool/CFG NINJA from any liability, claims, or damages arising from the security assessment and smart contract audit. It is recommended that the project owner consult legal counsel before entering into any agreement or contract.

