



Awaken

Security Assessment

CertiK Assessed on Aug 12th, 2025





Certik Assessed on Aug 12th, 2025

Awaken

The security assessment was prepared by Certik, the leader in Web3.0 security.

Executive Summary

TYPES

DeFi

ECOSYSTEM

Binance Smart Chain
(BSC)

METHODS

Formal Verification, Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Delivered on 08/12/2025

KEY COMPONENTS

N/A

CODEBASE

TokenSwap.sol

SHA256:

fc9daabd10397eb5bf3a510c2a10f2bf2f182bc664f223dbd40e2d7eb023

[View All in Codebase Page](#)

Vulnerability Summary



5

Total Findings

2

Resolved

0

Partially Resolved

3

Acknowledged

0

Declined



1

Centralization

1 Acknowledged



Centralization findings highlight privileged roles & functions and their capabilities, or instances where the project takes custody of users' assets.



0

Critical

Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.



0

Major

Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.



2

Medium

2 Acknowledged



Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.



1

Minor

1 Resolved



Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.



1

Informational

1 Resolved



Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | AWAKEN

Summary

[Executive Summary](#)

[Vulnerability Summary](#)

[Codebase](#)

[Audit Scope](#)

[Approach & Methods](#)

Review Notes

[Overview](#)

[External Dependencies](#)

[Privileged Functions](#)

Findings

[AWA-04 : Centralization Risks](#)

[AWA-01 : Mismatch in Token Amounts from Ignoring Decimal Differences in Swaps](#)

[AWA-03 : Lack of Exchange Rate Control Enables Arbitrage and Liquidity Drain](#)

[AWA-05 : Unprotected Upgradeable Contract](#)

[AWA-02 : Missing Emit Events](#)

Appendix

Disclaimer

CODEBASE | AWAKEN

Repository

TokenSwap.sol

SHA256: fc9daabd10397eb5bf3a510c2a10f2bf2f182bc664f223dbd40e2d7eb023b3ef

AUDIT SCOPE | AWAKEN

1 file audited ● 1 file without findings

ID	Repo	File	SHA256 Checksum
● TSC	CertiKProject/certik-audit-projects	 TokenSwap.sol	fc9daabd10397eb5bf3a510c2a10f2bf2f182 bc664f223dbd40e2d7eb023b3ef

APPROACH & METHODS | AWAKEN

This report has been prepared for Awaken to discover issues and vulnerabilities in the source code of the Awaken project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Formal Verification, Manual Review, and Static Analysis techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

REVIEW NOTES | AWAKEN

Overview

The **StableTokenSwap** contract is a lightweight, upgradeable smart contract designed to facilitate direct token-to-token swaps between two predefined ERC20 assets. It enables 1:1 exchanges without price calculation logic, relying instead on equal-value tokens and pre-funded liquidity.

External Dependencies

The contract relies on the following trusted libraries and standards:

- **@openzeppelin/contracts-upgradeable:**
 - `OwnableUpgradeable` : For basic administrative access control.
 - `ReentrancyGuardUpgradeable` : Prevents reentrant calls on sensitive functions.
 - `SafeERC20Upgradeable` : Ensures secure token interactions and checks return values for non-standard ERC20 tokens.
 - `Initializable` : Supports upgradeable proxy patterns by replacing constructors.

All dependencies are widely audited, trusted, and assumed to be configured correctly. The contract assumes that `tokenA` and `tokenB` conform to the standard ERC20 interface.

Privileged Functions

The contract includes several privileged functions restricted to the owner via `onlyOwner`:

- `setEnableA2B(bool enabled)` Enables or disables swaps from `tokenA` to `tokenB`. This gives the owner the ability to pause or resume one direction of exchange.
- `setEnableB2A(bool enabled)` Enables or disables swaps from `tokenB` to `tokenA`.
- `withdraw(address token, uint256 amount)` Allows the owner to withdraw arbitrary ERC20 tokens (including liquidity reserves) from the contract.

While these functions provide operational flexibility and safety controls, they also introduce centralization risks.

FINDINGS | AWAKEN



5

Total Findings

0

Critical

1

Centralization

0

Major

2

Medium

1

Minor

1

Informational

This report has been prepared to discover issues and vulnerabilities for Awaken. Through this audit, we have uncovered 5 issues ranging from different severity levels. Utilizing the techniques of Formal Verification, Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
AWA-04	Centralization Risks	Centralization	Centralization	● Acknowledged
AWA-01	Mismatch In Token Amounts From Ignoring Decimal Differences In Swaps	Inconsistency, Logical Issue	Medium	● Acknowledged
AWA-03	Lack Of Exchange Rate Control Enables Arbitrage And Liquidity Drain	Design Issue	Medium	● Acknowledged
AWA-05	Unprotected Upgradeable Contract	Logical Issue	Minor	● Resolved
AWA-02	Missing Emit Events	Coding Style	Informational	● Resolved

AWA-04 | CENTRALIZATION RISKS

Category	Severity	Location	Status
Centralization	Centralization	TokenSwap.sol (20250729-TokenSwap): 79, 83, 96	Acknowledged

Description

In the contract `StableTokenSwap` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority.

- `setEnableA2B(bool)` and `setEnableB2A(bool)`: These functions allow the owner to arbitrarily enable or disable swap directions (tokenA -> tokenB and vice versa). This introduces potential denial-of-service vectors, especially if users rely on bidirectional liquidity access.
- `withdraw(address token, uint256 amount)`: The owner can withdraw any amount of either token from the contract, regardless of whether that token is needed to maintain liquidity for active swaps. If misused, this could render the contract illiquid or expose users to unexpected failures.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign ($\frac{2}{3}$, $\frac{3}{5}$) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
OR
- Remove the risky functionality.

Alleviation

[Awaken, 08/01/2025]: The team acknowledged the issue and decided to add a timelock contract to mitigate centralization risks in the current engagement.

[CertiK , 08/08/2025] It is suggested to implement the aforementioned methods to avoid centralized failure. Also, CertiK strongly encourages the project team to periodically revisit the private key security management of all addresses related to centralized roles.

AWA-01 | MISMATCH IN TOKEN AMOUNTS FROM IGNORING DECIMAL DIFFERENCES IN SWAPS

Category	Severity	Location	Status
Inconsistency, Logical Issue	● Medium	TokenSwap.sol (20250729-TokenSwap): 49~50	● Acknowledged

Description

The `exchange` function in the `StableTokenSwap` contract does not account for the different decimal places between `tokenA` and `tokenB`. Tokens in the ERC20 standard can have varying decimals (e.g., USDT might have 6 decimals, while ETH has 18 decimals).

This discrepancy can lead to incorrect token amounts being exchanged, as the contract assumes both tokens have the same decimal precision. As a result, the contract might transfer an incorrect amount of the `toToken`, causing inconsistencies in the swap and potentially causing financial losses to users.

Recommendation

To address this issue, the `exchange` function should be modified to account for the differing decimal places between `tokenA` and `tokenB`.

Alleviation

[Awaken, 08/01/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

In our current design, both tokens are required to have fixed and matching decimals, so this issue does not apply under the intended deployment scenario.

AWA-03 | LACK OF EXCHANGE RATE CONTROL ENABLES ARBITRAGE AND LIQUIDITY DRAIN

Category	Severity	Location	Status
Design Issue	● Medium	TokenSwap.sol (20250729-TokenSwap): 73~74	● Acknowledged

Description

The exchange() function allows users to swap between two stablecoins (tokenA and tokenB) at a 1:1 ratio, assuming both tokens maintain equivalent value. However, this implementation lacks any rate validation or external pricing reference, introducing two potential issues:

Arbitrage Opportunity: If tokenA and tokenB diverge in real-world value (e.g., 0.98 vs 1.00), users can exploit the fixed 1:1 rate to profit by swapping the overvalued token for the undervalued one. Repeating this process could result in net asset loss for the contract.

Liquidity Drain Risk: Even without a price gap, a malicious or opportunistic user can convert all of one token into the other, completely depleting liquidity for one side of the swap. This renders future swaps in that direction unavailable, disrupting the contract's intended function.

Recommendation

To mitigate the risk while keeping the swap model simple:

Integrate an Oracle: Use a trusted price oracle (e.g., Chainlink) to enforce real-time fair exchange rates between tokenA and tokenB. This helps avoid arbitrage by only allowing swaps close to the actual market value.

Apply an Amount Limiter: Introduce per-user or per-transaction limits to restrict how much can be swapped in a single call. This reduces the impact of sudden liquidity depletion and gives the system time to rebalance if needed.

Alleviation

[Awaken, 08/01/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

The design of this contract enforces a fixed 1:1 exchange rate, which does not change based on market price fluctuations. Moreover, to deal with extreme arbitrage situations: To mitigate extreme scenarios, we plan to implement per-transaction limits and overall liquidity safeguards to prevent total depletion.

AWA-05 | UNPROTECTED UPGRADEABLE CONTRACT

Category	Severity	Location	Status
Logical Issue	Minor	TokenSwap.sol (20250729-TokenSwap): 31	Resolved

Description

The `StableTokenSwap` logic contract does not protect the initializer. An attacker can front-run the `initialize` call and assume ownership of the logic contract. Once in control, the attacker can perform privileged operations, misleading users into believing that they are interacting with the legitimate owner of the upgradeable contract.

Recommendation

We recommend adding

```
/// @custom:oz-upgrades-unsafe-allow constructor
constructor() initializer {...}
```

OR

```
/// @custom:oz-upgrades-unsafe-allow constructor
constructor() {
    ...
    _disableInitializers();
}
```

This addition will prevent the function `require()` from being called directly in the implementation contract, but the proxy will still be able to initialize its storage variables.

Alleviation

[Awaken, 08/01/2025]: The team heeded the advice and resolved the issue by restricting initialization permissions in commit [a20ef5487511295cadf92dc943256d24772e8dfc](https://github.com/TokenSwap/TokenSwap/commit/a20ef5487511295cadf92dc943256d24772e8dfc).

AWA-02 | MISSING EMIT EVENTS

Category	Severity	Location	Status
Coding Style	● Informational	TokenSwap.sol (20250729-TokenSwap): 79, 83	● Resolved

Description

There should always be events emitted in sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended to emit events in sensitive functions that are controlled by centralization roles.

Alleviation

[Awaken, 08/01/2025]: The team heeded the advice and resolved the issue by our recommendations in commit [615d911ef76bd5d490b317596e847c34aa398d33](https://github.com/TokenSwap/TokenSwap/commit/615d911ef76bd5d490b317596e847c34aa398d33).

APPENDIX | AWAKEN

Finding Categories

Categories	Description
Coding Style	Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable.
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. 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. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR 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, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'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. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

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

Elevating Your Entire **Web3** Journey

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

