QuillAudits

AUDIT REPORT

May , 2025

For

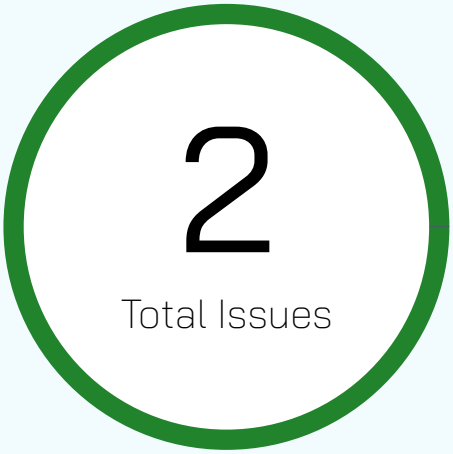
Demex

Table of Content

Executive Summary

Project name	Demex
Project URL	https://dem.exchange/
Overview	This contract enables 1:1 migration of SWTH tokens to DMX tokens by burning SWTH (sent to address(0)) and transferring pre-deposited DMX.
Audit Scope	The scope of this Audit was to analyze the Demex Smart Contracts for quality, security, and correctness. https://github.com/Switcheo/carbon-axelar-evm/blob/main/src/SwthToDmxMigrator.sol
Contracts in Scope	SwthToDmxMigrator.sol
Commit Hash	7d07e0fe4e84f509eaa3a75391d5d3ca6d98aba7
Language	Solidity
Blockchain	Ethereum
Method	Manual Analysis, Functional Testing, Automated Testing
Review 1	8th May 2025
Updated Code Received	12th May 2025
Review 2	12th May 2025
Fixed In	166608a50b65cbf4b9d0a81b5c67a9ed18c8dbf1

Number of Issues per Severity



High	0 (0.00%)
Medium	0 (0.00%)
Low	2 (100.00%)
Informational	0 (0.00%)

Severity

Issues	High	Medium	Low	Informational
Open	0	0	0	0
Resolved	0	0	**2**	0
Acknowledged	0	0	0	0
Partially Resolved	0	0	0	0

Checked Vulnerabilities

- ✓ Access Management
- ✓ Arbitrary write to storage
- ✓ Centralization of control
- ✓ Ether theft
- ✓ Improper or missing events
- ✓ Logical issues and flaws
- ✓ Arithmetic Computations Correctness
- ✓ Race conditions/front running
- ✓ SWC Registry
- ✓ Re-entrancy
- ✓ Timestamp Dependence
- ✓ Gas Limit and Loops
- ✓ Exception Disorder
- ✓ Gasless Send
- ✓ Use of tx.origin
- ✓ Malicious libraries
- ✓ Compiler version not fixed
- ✓ Address hardcoded
- ✓ Divide before multiply
- ✓ Integer overflow/underflow
- ✓ ERC's conformance
- ✓ Dangerous strict equalities
- ✓ Tautology or contradiction
- ✓ Return values of low-level calls
- ✓ Missing Zero Address Validation
- ✓ Private modifier
- ✓ Revert/require functions
- ✓ Multiple Sends
- ✓ Using suicide
- ✓ Using delegatecall
- ✓ Upgradeable safety
- ✓ Using throw

- [x] Using inline assembly
- [x] Unsafe type inference
- [x] Style guide violation
- [x] Implicit visibility level

Techniques and Methods

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

- The overall quality of code.
- Use of best practices.
- Code documentation and comments, match logic and expected behavior.
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Implementation of ERC 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 analyzed 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

A 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 analyzed, 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 behavior 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, Foundry, Solhint, Mythril, Slither, Solidity statistical analysis.

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below

High Severity Issues

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 Severity Issues

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 Severity Issues

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

Informational Issues

These are four 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

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

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.

Low Severity Issues

Use Two-Step Ownership Transfer

Resolved

Path

SwthToDmxMigrator.sol

Description

This contract currently implements a basic single-step ownership transfer through OpenZeppelin's Ownable, which presents a serious security vulnerability. In the existing setup, if the current owner accidentally specifies an incorrect address during an ownership transfer - whether due to a typographical error, copy-paste mistake, or address corruption - the contract ownership would immediately and irreversibly shift to that address.

This dangerous single-point failure could permanently lock out legitimate administrators, as there would be no cancellation mechanism or recovery process available. The consequences would be severe: all owner-restricted functions, including the critical transferToken method, would become permanently inaccessible if ownership is transferred to an invalid or non-responsive address.

Recommendation

Use OpenZeppelin's Ownable2Step instead of Ownable

Missing Safety Check Before Token Transfer

Resolved

Path

SwthToDmxMigrator.sol

Function

migrateFromSwthToDmx

Description

The transferSwth() function does not verify whether the contract has sufficient DMX balance before burning the user's SWTH tokens. While safeTransfer would revert on failure, a pre-check would provide clearer error messaging and prevent unnecessary gas waste from partial execution.

Recommendation

Add an explicit balance check

Functional Tests

Some of the tests performed are mentioned below:

- transferSwth function works as expected
- migrateFromSwthToDmx function should also work as expected but its description is incomplete
- Assume that the contract is not able to migrate the customized amount

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 Demex. We performed our audit according to the procedure described above.

Two issues of Low severity were found. Demex team resolved them all

Disclaimer

At QuillAudits, we have spent years helping projects strengthen their smart contract security. However, security is not a one-time event—threats evolve, and so do attack vectors. Our audit provides a security assessment based on the best industry practices at the time of review, identifying known vulnerabilities in the received smart contract source code.

This report does not serve as a security guarantee, investment advice, or an endorsement of any platform. It reflects our findings based on the provided code at the time of analysis and may no longer be relevant after any modifications. The presence of an audit does not imply that the contract is free of vulnerabilities or fully secure.

While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

Stay proactive. Stay secure.

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

7+ Years of Expertise	**1M+** Lines of Code Audited
$30B+ Secured in Digital Assets	**1400+** Projects Secured

Follow Our Journey

AUDIT REPORT

May , 2025

For

Demex

QuillAudits

Canada, India, Singapore, UAE, UK
www.quillaudits.com audits@quillaudits.com