WHITE HAT DAO

Dyl Token

Safety Rating

In quest of web3 safety
www.whitehatdao.com

Date: 10/01/2024

Table of Contents

Disclaimer

Executive Summary

Summary of Findings

Introduction
- Project Summary
- Project Scope
- Audit Details
- Methodology

Findings
- Severity Definitions
- Critical Vulnerabilities
- Major Vulnerabilities
- Medium Vulnerabilities
- Low Vulnerabilities

Conclusion

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report.

In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions.

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and White Hat DAO and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives)

White Hat DAO owes no duty of care towards you or any other person, nor does White Hat DAOmake any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and White Hat DAOhereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report.

Except and only to the extent that it is prohibited by law, White Hat DAOhereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against White Hat DAO, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security.

No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

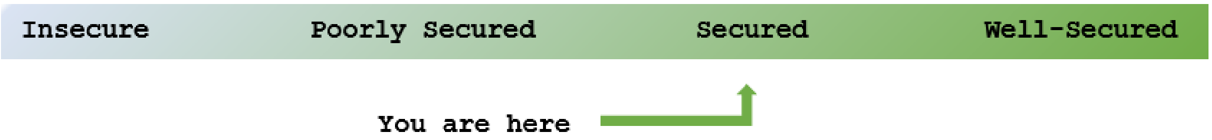
We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Executive Summary

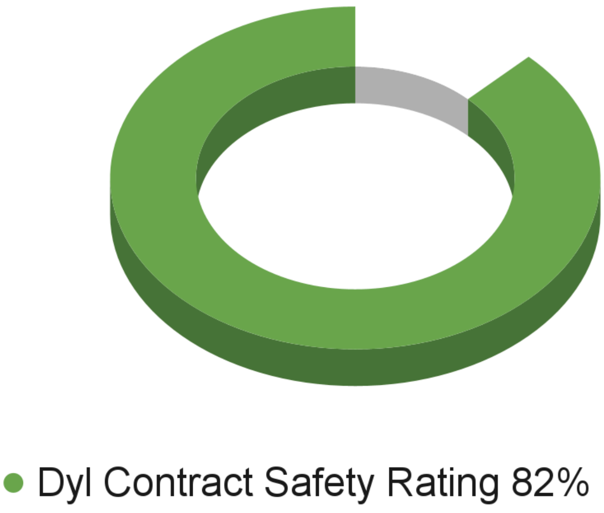
White Hat DAO has conducted this security assessment.   There was 1 contract reviewed during this security assessment. The smart contract was manually reviewed and analyzed with static and dynamic analysis tools.

Based on our examination, the contract is Secured.



No major issues related to the codebase were found. Although improvement can be made. More details have been provided as below.

Safety Score: 82%



Introduction

This security assessment has been prepared for Dyl Contract by WHD to find any safety concerns, bad practices and vulnerabilities in the source code as well as any contract dependencies in scope that were not part of an officially recognized library. Comprehensive tests have been conducted, utilizing manual code review, static and dynamic analysis and techniques.

The 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
- Reviewing unit tests to ensure full coverage of the codebase

The Project Summary, Scope, Details and Methodology of the assessment is described in the following sections.

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. These can be found in the Findings section of the report.

Project Summary

Project	Dyl Token
Description	Dylan Rhodes, known as Dyl is a Multi-Platinum awarded recording artist and entrepreneur from Philadelphia, PA. Dyl is a pioneer of crypto and Music NFTs
Website	https://dylmusic.com
Platform	Ethereum
Language used	Solidity
Codebase	https://etherscan.io/address/0x7a8946eda77817126ffe301249f6dc4c7df293c3#code
Commit	

Project Scope

White Hat DAO was commissioned by Dyl to perform security assessments on smart contracts as below:

Source Code	Acknowledgement	nSloc
https://etherscan.io/address/0x7a8946eda77817126ffe301249f6dc4c7df293c3#code	Accepted	

Details

Delivery Date	10/01/2024
Submission Date	09/01/2024
Key Components	Dyl Token

Methodology

Code review was conducted on following source-code
https://etherscan.io/address/0x7a8946eda77817126ffe301249f6dc4c7df293c3#code)

The code was manually reviewed in an attempt to identify potential vulnerabilities and verify adherence to the specification, best practices and proper use of the language itself. The unit tests were examined to ensure full coverage of the code. Automated analysis of the codebase was performed and results were reviewed.

The smart contracts were scanned for commonly known and more specific vulnerabilities. Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Access Control
- Arbitrary token minting
- Asset's integrity
- Authority Control attack
- Business Logics Review
- Centralization of power
- Client synchronization
- Code clones, functionality duplication
- Conditional Completion attack

- Consensus splits
- Costly Loop
- Data Consistency
- Data integrity loss
- Denial of service / logical oversights
- Deployment Consistency
- DoS with (Unexpected) Throw
- DoS with Block Gas Limit
- ERC20 API violation
- Escrow manipulation
- Explicit visibility of functions state variables
- False top-up Vulnerability
- Falsified messages
- Floating Points and Numerical Precision
- Functionality Checks
- Gas Usage, Gas Limit and Loops
- Implicit visibility level
- Injection type attacks
- Integer Overflow and Underflow attacks
- Invalid incoming messages
- Kill-Switch Mechanism
- Logic Flaws
- Mishandled exceptions and call stack limits
- Number rounding errors
- Operation Trails & Event Generation
- Outdated data in cache
- Ownership Takeover
- Redundant fallback function
- Reentrancy
- Remote code execution
- Reordering attack
- Replay attacks
- Repository Consistency
- Scoping and Declarations

- Second pre-image attacks on Merkle Trees
- Short address attack
- Style guide violation
- TimeStamp Dependence attack
- Token Supply manipulation
- Transaction Ordering Dependence attack
- tx.origin Authentication
- Unchecked external call
- Unchecked math
- Uninitialized Storage Pointers
- Unsafe external calls
- Unsafe type Inference
- User Balances manipulation

Severity Definitions

Severity	Definitions
Critical	These vulnerabilities have a catastrophic impact on the security of the project. They can lead to loss, data manipulation, take over, etc. It is strongly recommended to fix these vulnerabilities.
High	These vulnerabilities have a significant impact on the security of the project. They can lead to loss, data manipulation, take over, etc. It is strongly recommended to fix these vulnerabilities.
Medium	These vulnerabilities are important to fix. These vulnerabilities alone can't lead to asset loss or data manipulation. However, medium vulnerabilities can be chained to create a more severe vulnerability. It is highly recommended to review and address these vulnerabilities.
Low	These vulnerabilities are mostly related to outdated, unused code snippets and don't have significant impact on execution. It is suggested that the project party evaluate and consider whether these vulnerabilities need to be fixed.
Informational	These vulnerabilities don't pose an immediate risk, but are relevant to security best practices. They could be code style violations and informational statements that don't affect smart contract execution. They may be able to be ignored.

Critical Vulnerabilities

No Low severity / vulnerabilities were found.

Major Vulnerabilities

No Major severity / vulnerabilities were found.

Minor Vulnerabilities

No Minor severity / vulnerabilities were found.

However no harmful vulnerabilities were found, it is worth to mention that

# Contract was not renounced

# No LP Burnt / Locked - Locking or burning LP provides community safety to prevent owner from directly removing LP from the pool.
LP Contract - 0x1f98431c8ad98523631ae4a59f267346ea31f984 (Univ3)

# Contract Complies - yes

# Honeypot test - Passed

# Contract controlled by proxy - No

# Contract by known scam wallet

# Potential Multi-Blacklist- No

# Can Whitelist- No

# Can Update Taxes/Fees - No

# Can Update Max Wallet - No

# Can Update Max Tx- No

# Can Pause Trading- No

# Trading Cooldown- No

#Can Update Fee Wallets - No

Conclusion

The code was commented well. Comments are helpful in understanding the overall architecture and the logic flow of the contracts.