MixBytes()

Audit

OF AKROPOLIS
TOKEN VESTING CONTRACTS

JULY 10
2019

FOREWORD
TO REPORT

A small bug can cost you millions. **MixBytes** is a team of experienced blockchain engineers that reviews your codebase and helps you avoid potential heavy losses. More than 10 years of expertise in information security and high-load services and 11 000+ lines of audited code speak for themselves.

This document outlines our methodology, scope of work, and results.

We would like to thank **Akropolis** for their trust and opportunity to audit their smart contracts.

CONTENT
DISCLAIMER

This report was made public upon consent of **Akropolis**. **MixBytes** is not to be held responsible for any damage arising from or connected with the report.

Smart contract security audit does not guarantee a comprehensive inclusive analysis disclosing all possible errors and vulnerabilities but covers the majority of issues that represent threat to smart contract operation, have been overlooked or should be fixed.

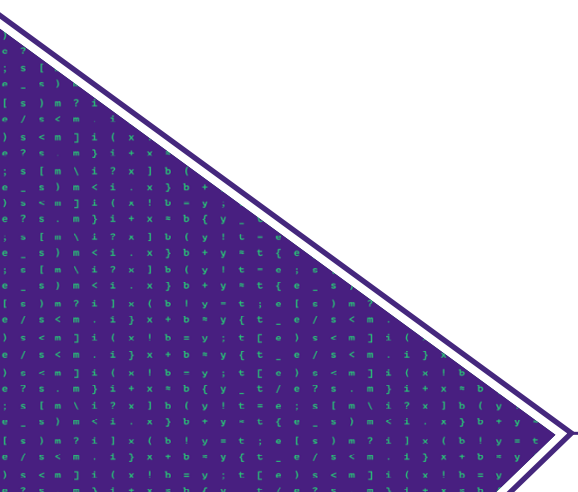

TABLE OF CONTENTS

01 INTRODUCTION TO THE AUDIT

GENERAL PROVISIONS

The **Akropolis** team asked **MixBytes Blockchain Labs** to audit their token vesting contracts.

SCOPE OF THE AUDIT

The primary scope of the audit is smart contracts at: **https://github.com/akropolisio/akropolis-vesting/tree/61b9b6cb107593e614aa9f9105d8c2a7a3edd65a/contracts**.

02 SECURITY ASSESSMENT PRINCIPLES

CLASSIFICATION OF ISSUES

CRITICAL

Bugs leading to Ether or token theft, fund access locking or any other loss of Ether/tokens to be transferred to any party (for example, dividends).

MAJOR

Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.

WARNINGS

Bugs that can break the intended contract logic or expose it to DoS attacks.

COMMENTS

Other issues and recommendations reported to/acknowledged by the team.

SECURITY ASSESMENT METHODOLOGY

The audit was performed with triple redundancy by three auditors. Stages of the audit were as follows:

1. “Blind” manual check of the code and model behind the code
2. “Guided” manual check of the code
3. Check of adherence of the code to requirements of the client
4. Automated security analysis using internal solidity security checker
5. Automated security analysis using public analysers
6. Manual by-checklist inspection of the system
7. Discussion and merge of independent audit results
8. Report execution

03 DETECTED ISSUES

CRITICAL

None found.

MAJOR

None found.

WARNINGS

1. AkropolisVesting.sol#L28

It is still possible to call function `release` for the token despite `onlyBeneficiary` access modifier. It can be done via base contract function `release(IERC20 token) public`. This poses no security risk (see below). However, if this behaviour is undesired, we recommend to override `release(IERC20 token) public` function and add the access modifier.

Status:

FIXED - in commit **44199fc**

2. AkropolisVesting.sol#L28

In case of `release` function `onlyBeneficiary` modifier does not add extra security. The contract will transfer the funds only to the beneficiary according to the schedule in any case. The modifier only prevents the transfer transactions from being initiated by a third party. If the beneficiary is a multi-signature wallet, it may fail to call this function.

Status:

FIXED - in commit **44199fc**

3. AkropolisTimeLock.sol#L29

In case of `release` function `onlyBeneficiary` modifier does not add extra security. The contract will transfer the funds only to the beneficiary according to the time lock in any case. The modifier only prevents the transfer transaction from being initiated by a third party. If the beneficiary is a multi-signature wallet, it may fail to call this function.

Status:

FIXED - in commit **44199fc**

COMMENTS

None.

04 CONCLUSION AND RESULTS

Overall quality of the code is high. No security-related issues were discovered.

ABOUT MIXBYTES

MixBytes is a team of experienced developers providing top-notch blockchain solutions, smart contract security audits and tech advisory.

JOIN US

OUR CONTACTS

Alex Makeev
Chief Technical Officer

Vadim Buyanov
Project Manager