DeFiner FIN Token Smart Contract

Security Audit Report

September 11, 2020

Auditor: Alexander Remie

https://takasecurity.com

Table Of Contents

Executive Summary

DeFiner requested a security audit of the DeFiner FIN Token smart contract by Taka Security. The security audit focused on verifying that the token contract fully adheres to the ERC20 token standard. During the security audit performed by Taka Security on September 9/10 2020 no issues were discovered. The DeFiner FIN Token smart contract is fully compliant with the ERC20 token standard.

About

Taka Security is an Amsterdam-based company whose core business is offering Ethereum smart contract auditing services. Besides performing audits the company also works on the development of Ethereum smart contract analysis tools. The company was founded in 2020 by Alexander Remie.

Alexander is an independent Ethereum smart contract auditor who has previously worked for ChainSecurity and PwC Switzerland. After gaining experience doing dozens of audits for these companies he decided to set up his own Ethereum smart contract auditing company. Alexander has experience auditing various types of Ethereum smart contract projects: ranging from decentralized exchanges, tokens, DeFi projects, and projects based on ENS, amongst others. Before working as an Ethereum smart contract auditor Alexander worked in traditional payments and as an Ethereum smart contract developer.

Audit Overview

Timeline

Taka Security was contracted to perform a security audit of the DeFiner FIN token smart contract for the duration of 2 days. The audit was started on September 10, 2020. The public report was delivered to DeFiner on September 11, 2020.

Scope

Compiler version	0.6.2
Mainnet address	`0x054f76beed60ab6dbeb23502178c52d6c5debe40`

Review Methodology

During an audit Taka Security will execute Ethereum security analysis tools, as well as perform a thorough manual review. The manual review will focus on finding security related issues, as well as flagging bad practices or inefficient designs. If a specification is provided Taka Security will verify it reflects the implementation. Each issue found will be written into a separate finding in the report.

Findings Resolution

After the initial report has been sent to the client, it is up to the client to update the source code to resolve the reported findings. Once client has provided the updated source code to Taka Security, each resolved finding will be updated accordingly with a short description of the applied code changes.

Limitations

Security auditing cannot uncover all existing vulnerabilities: even a contract in which no vulnerabilities are found during the audit is not a guarantee of a secure smart contract. However, auditing enables the discovery of vulnerabilities that were overlooked during development and areas where additional security measures are necessary.

Terminology

Each finding is assigned one or more labels each describing a specific aspect of the finding.

Finding types

security Could cause actual problems with real consequences.

design Describes shortcomings of the current design.

note Describes further areas of concern or possible small improvements to the code.

Finding severities

critical Must be fixed.

high Highly recommended to fix.

medium Should be fixed.

low Could be fixed.

The severity of security findings depends on two ratings.

Impact How severe are the consequences of the issue being triggered.

Likelihood how likely is is that the finding is triggered. Either accidentally or on purpose by a malicious actor.

The following table describes the security finding severity according to the Likelihood and Impact rating.

	IMPACT		
LIKELIHOOD	High	Medium	Low
High	critical	high	medium
Medium	high	medium	low
Low	medium	low	low

Finding resolvement

When client provides fixes and/or explanations for how they addressed each finding one of the following labels is assigned to each finding.

FIXED The described finding has been fixed.

PARTIALLY FIXED The finding has been partially fixed.

ACKNOWLEDGED Client acknowledged the issue but has decided to not update the code due to certain reasons.

Findings that have not bee fixed and no reason has been provided are not assigned any of the above labels.

Project Overview

The DeFiner FIN Token smart contract implements an ERC20 token built on top of the OpenZeppelin `ERC20.sol` smart contract. The total supply of tokens is minted to the deployer address in the constructor. After deployment it is not possible to mint new tokens, i.e. the total supply static.

Token Info

Token standard(s)	ERC20
Name	DeFiner
Symbol	FIN
Decimals	18
Total supply	168,000,000
Pausable	no
Mintable	no
Burnable	no
Upgradable	no

Roles

There are no privileged roles.

Findings

This section lists the issues found during the audit of the DeFiner FIN Token smart contracts.

Taka Security did not find any issues.

Disclaimer

UPON REQUEST BY DEFINER, TAKA SECURITY AGREES TO MAKE THIS AUDIT REPORT PUBLIC. THE CONTENT OF THIS AUDIT REPORT IS PROVIDED “AS IS”, WITHOUT REPRESENTATIONS AND WARRANTIES OF ANY KIND, AND TAKA SECURITY DISCLAIMS ANY LIABILITY FOR DAMAGE ARISING OUT OF, OR IN CONNECTION WITH, THIS AUDIT REPORT. COPYRIGHT OF THIS REPORT REMAINS WITH TAKA SECURITY.

Contact:

https://takasecurity.com
contact@takasecurity.com