decurity

Security audit proposal

By Decurity
For Asterizm

Contents

Recent Hacks

2023 - $1.5+ billion
2024 - $1.1+ billion
(loss of users' funds)

Euler Finance - REKT
$197,000,000 | 03/13/2023

Hedgey Finance - Rekt
$44,700,000 | 04/19/2024

Sonne Finance - Rekt
$20,000,000 | 05/15/2024

ZKasino - Rekt
$33,000,000 | 04/20/2024

Introduction

$15 000 000

Rescued directly by our team

80+

Audits delivered since 2022

Security Audit reports by Decurity

Omar Ganiev

(CEO)

- *Cybersecurity enthusiast since 2007*
- *Entrepreneur, winner of numerous CTF competitions, penetration tester and web3 security auditor, speaker and author*

Arseniy Reutov

(CTO)

- *Speaker at DEFCON, AppSec California, OWASP London, ETHDubai, TrustX*
- *Author of research papers on application security since 2008, developer of popular open-source tools for blockchain security*

Top-notch hackers at your service

Top-2 in Paradigm CTF 2022

Top-2 in OpenZeppelin CTF 2024

- **Team experience**

  We employ full-stack web3 hackers with vast experience both in blockchain and traditional financial systems such as banks and payment gateways.

- **Network**

  We've provided security reviews for multiple DeFi projects including Compound, Zircuit, 1inch, Yearn, Gearbox, GIVEth, Symbiosis Finance, Ether Fi, and also audited Layer 1 blockchains including NEM, Waves, Symbol, BitClout, and others (Security Audit reports by Decurity).

- **Achievements**

  We've scored 2nd places in both some of the hardest smart contract security audit competitions – Paradigm CTF 2022 and OpenZeppelin CTF 2024.

- **Authorship**
  - Fuzzy differ for the DeFi codebases contract-diff.xyz
  - Semgrep SAST rulepack for Solidity vulnerability scanning: Semgrep rules for smart contracts based on DeFi exploits
  - The function signature bruteforcer: GitHub - Decurity/abi-decompiler: Ethereum (EVM) smart contracts reverse engineering helper utility

- **Developing**

  We are developers of DeFiMon — real-time on-chain hack detection product. We post some of the alerts on X: Decurity (@DecurityHQ) / X.

- **Publishing**

  We have a few research write-ups in our blog https://blog.decurity.io/ including the $5M critical bug disclosure and the AMM, CDP, and LSD auditing checklists.

Trusted by



ether.fi 1inch Symbiosis



Compound Zircuit SOCKET


Gearbox zkBob



Yearn

Scope of work

This document contains a security audit service proposal made by Decurity for Asterizm (hereinafter referred to as the "Customer").

Company info:

- Name: Decentralized Security LLC-FZ (Decurity).
- Website: https://decurity.io/.
- Email: sales@decurity.io.

Tasks solved during the work are:

- Review the protocol design and the usage of 3rd party dependencies,
- Audit the implementation of the contracts,
- Develop recommendations and suggestions to improve the security of the contracts.

The audit scope includes the contracts in the following repository:
EVM: https://github.com/Asterizm-Protocol/asterizm-contracts-evm
SOLANA: https://github.com/Asterizm-Protocol/asterizm-contracts-sol
TON: https://github.com/Asterizm-Protocol/asterizm-contracts-ton

Terms of work

Option 1

Stage	Workload/Time	Price	Result
Security Audit EVM + TVM	15 business days A team of **4** senior researchers	~~**60 000 USD**~~ 35 000 USD	• Fixed vulnerabilities • Improved security • **Official Security Audit Report**
Security Audit SOL	15 business days A team of **4** senior researchers	~~**60 000 USD**~~ 40 000 USD	
Mitigation verification of the previously identified issues	5 business days	0 USD	• Fixes validation • **Updated Security Audit Report**

The updates are to be provided weekly in an informal way via online chat or email. The final report will contain an executive summary and detailed description of all the discovered weaknesses along with remediation recommendations.

Payment options: USDT/USDC (ERC/TRC), wire transfer.

This offer is valid until **Oct 18, 2024**.

The closest preferred slots for booking are starting on **Oct 14, 2024** and **Oct 21, 2024**.

Option 2

Stage	Workload/Time	Price	Result
Security Audit EVM + TVM + SOL	30 business days A team of **8** senior researchers	~~**75 000 USD**~~ 60 000 USD	• Fixed vulnerabilities • Improved security • Reduced risk of hacks • **Official Security Audit Report**
Re-testing	5 business days	0 USD	• Remediation validation • **Updated Security Audit Report**
		~~**75 000 USD**~~ **60 000 USD**	

The updates are to be provided weekly in an informal way via online chat or email. The final report will contain an executive summary and detailed description of all the discovered weaknesses along with remediation recommendations.

Payment options: USDT/USDC (ERC/TRC), Wire transfer.

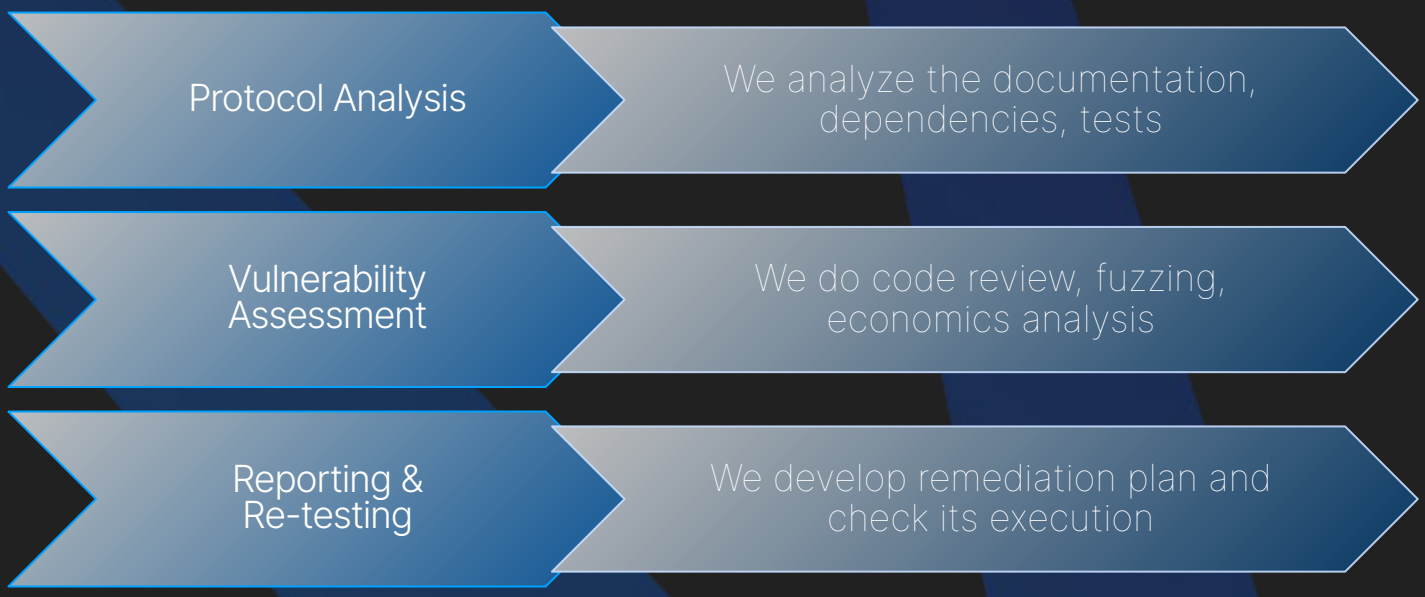
This offer is valid until **Oct 18, 2024**.

The closest preferred slots for booking are starting on **Oct 14, 2024** and **Oct 21, 2024**.

Description of work

The audit will follow well-known application security testing methodologies and implement checks specific to DeFi and smart contract security.

The diagram below shows the key stages of the security audit:



The high-level steps are as follows:

1. Protocol analysis
    1.1. Reconnaissance of the contracts, 3rd party libraries, external dependencies, and interfaces in the scope,
    1.2. Contract diffing and identification of the code reuse,
    1.3. Documentation and intended business logic analysis,
    1.4. Study of the previous audits if available,
    1.5. Contract tests analysis if available.
2. Vulnerability assessment
    2.1. Automated static analysis for the low-hanging fruits,
    2.2. Manual deep analysis of code-specific weaknesses such as insufficient access control or susceptibility to reentrancy,
    2.3. Manual deep analysis of DeFi-specific weaknesses such as susceptibility to front-running or flash loan manipulations,
    2.4. Setting up the fuzzing invariants if applicable, running the fuzzing tests, and verifying the results.
3. Exploitation
    3.1. Development of potential attack vectors for the identified weaknesses,
    3.2. Development of test scripts for proof of concept attacks on the forks of blockchain.
4. Reporting
    4.1. Risk analysis of the validated weaknesses and vulnerabilities,
    4.2. Development of recommendations relevant to the codebase and the protocol's limitations,
    4.3. Writing the executive summary and detailed description of the findings.
5. Finalization
    5.1. Optional retesting after appropriate patches are implemented
    5.2. Updating the status of vulnerabilities in the report.

Apart from the report, if requested, we can provide audit artifacts such as developed unit tests, the output of the automated analysis and fuzzing tools, the breakdown of the contract methods and attributes, etc.

Legal

The company's legal entities are "Continuous Technologies Global Inc." in the USA and "Decentralized Security LLC-FZ" in the UAE.

Social

Our website and research blog:

- https://decurity.io/
- https://blog.decurity.io/