HackSafe

Smart Contract Security Audit Report

GOVI

November 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
GOVI

Deployer address
0xCedAD8C0Ae5e0a878c01cC8c81E0Ca2DbA909deD

Client contacts
GOVI Team

Blockchain
Ethereum

Website
https://cvi.finance/

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. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make 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 HackSafe hereby 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by GOVI to perform an audit of smart contracts:

- https://etherscan.io/token/0xeeaa40b28a2d1b0b08f6f97bb1dd4b75316c6107#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 08.11.2022

Token Type	: ERC20
Contract name	: GOVI
Contract address	: 0xeEAA40B28A2d1b0B08f6f97bB1DD4B75316c6107
Total supply	: 32,000,000
Token Ticker	: GOVI
Decimals	: 18
Token Holders	: 3,123
Transactions count	: 61,390
Compiler version	: v0.6.12+commit.27d51765
Contract deployer address	: 0xCedAD8C0Ae5e0a878c01cC8c81E0Ca2DbA909deD
Owner address	: 0xCedAD8C0Ae5e0a878c01cC8c81E0Ca2DbA909deD

Social profiles

Twitter Profile	: https://twitter.com/official_cvi
Coinmarketcap Profile	: https://coinmarketcap.com/currencies/govi/
Coingecko profile	: https://www.coingecko.com/en/coins/govi/
Telegram profile	: https://t.me/cviofficial
Github profile	: https://github.com/coti-io/cvi-contracts

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Well Secure”.** This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.

Insecure	Poor secured	Secure	Well-secured

You are here

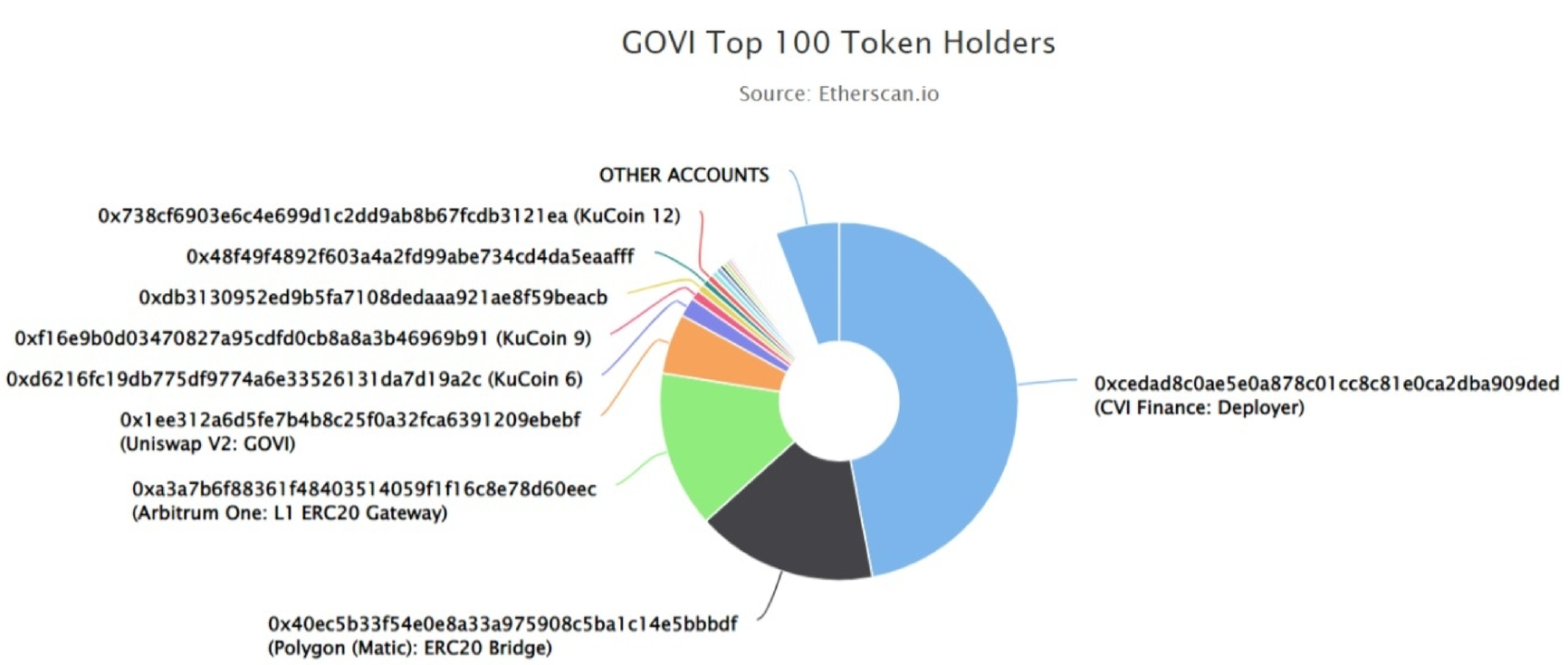
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 1 low.

GOVI Token Distribution

The top 100 holders collectively own 94.23% (30,154,382.07 Tokens) of GOVI

Token Total Supply: 32,000,000.00 Token | Total Token Holders: 3,123



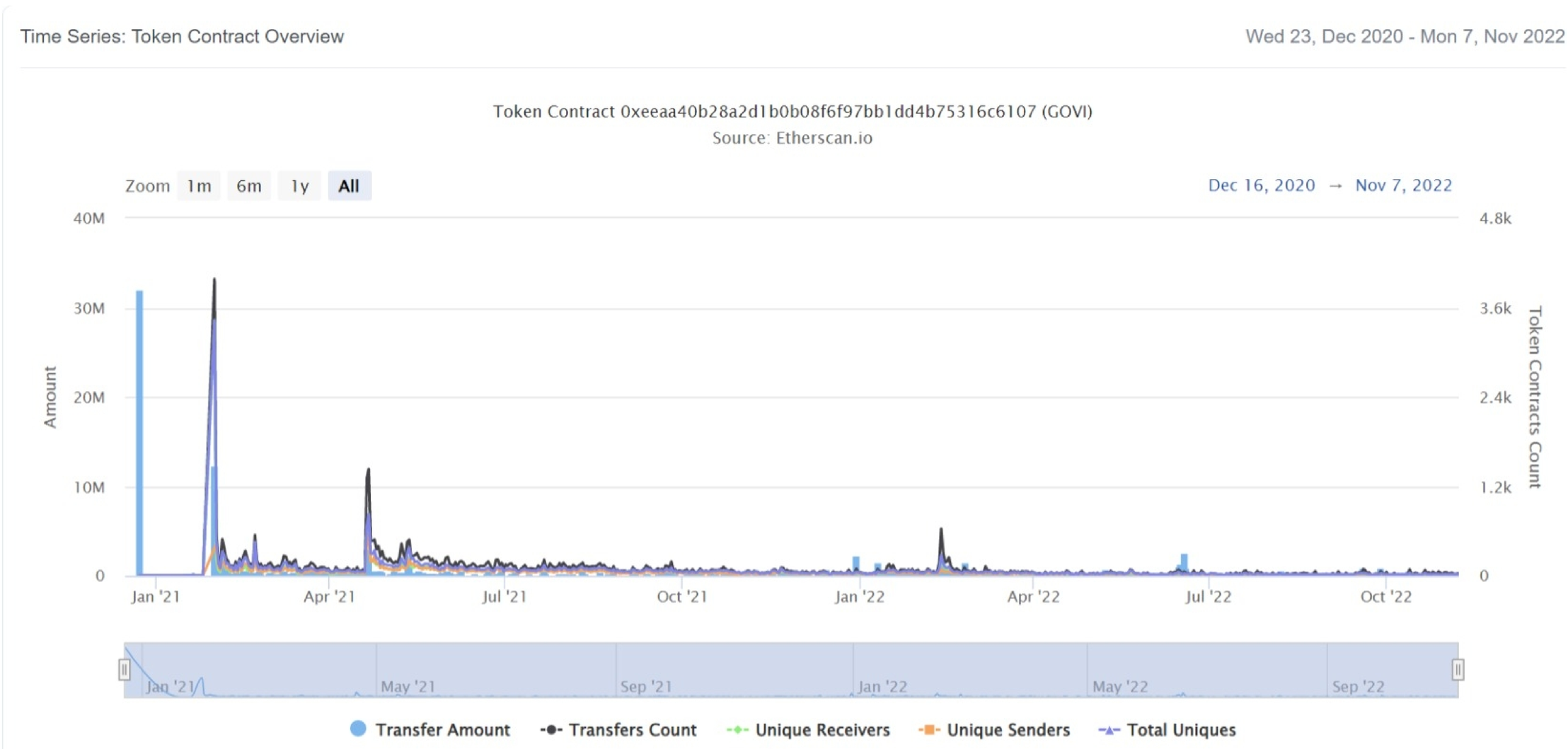
GOVI Token Top 20 Token Holders

(A total of 30,154,382.07 tokens held by the top 100 accounts from the total supply of 32,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	CVI Finance: Deployer	15,049,854	47.0308%
2	Polygon (Matic): ERC20 Bridge	5,216,655.707537914124882062	16.3020%
3	Arbitrum One: L1 ERC20 Gateway	4,537,036.982063919246350823	14.1782%
4	Uniswap V2: GOVI	1,742,918.160898241941628126	5.4466%
5	KuCoin 6	559,510.966216758898304708	1.7485%
6	KuCoin 9	279,779.476712952152826645	0.8743%
7	0xdb3130952ed9b5fa7108dedaaa921ae8f59beacb	216,989.761298790199721738	0.6781%
8	0x48f49f4892f603a4a2fd99abe734cd4da5eaafff	189,036.930441158182454262	0.5907%
9	KuCoin 12	185,152.671707168143269216	0.5786%
10	SushiSwap: GOVI	165,094.268511632336327992	0.5159%
11	0x86626ff0b721713c473aa54e9436da26191f22f6	150,000	0.4688%
12	0x936dd3112a9d39af39adda798503d9e7e7975fb7	109,523.743197709214234749	0.3423%
13	0x352f2123f79a1a7a77cdad5eba80f05c42360fc0	104,346.1063	0.3261%
14	0x7282bdf045bb0aaf2fdcad6ea9f39a2204c9a023	95,788.20894	0.2993%
15	0x93337cce0f3f2e3236772859609d1bdcaeb8f5a9	76,605	0.2394%
16	0x49dd1c8595fe34be8213ba97662992ca23cef5b0	59,883.5449	0.1871%
17	0x7f25b76932ca2ad171f4addb5eb190c47c11fc43	58,976.005295086650972073	0.1843%
18	0x118453bb70f9cf1a05e805069d7e393bec045833	57,928.603246810518472065	0.1810%
19	0xc742f7aa9390bd00d79966e9f2514d5384bb0e6c	50,000	0.1563%
20	0x926bf90196781cf2161535d48af542889cac4d2e	42,388.742027711967338545	0.1325%

GOVI Token Distribution

GOVI Token Contract Overview



Contract functions details

+[Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+[Lib] SafeMath
    -[Int] add
    -[Int] sub
    -[Int] sub
    -[Int] mul
    -[Int] div
    -[Int] div
    -[Int] mod

+[Lib] Address
    -[Int] isContract
    -[Int] sendValue
    -[Int] functionCall
    -[Int] functionCall
    -[Int] functionCallWithValue
    -[Int] functionCallWithValue
    -[Pvt] _functionCallWithValue

+ERC20 (Context, IERC20)
    -[Pub] <constructor>
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer #
    -[Pub] allowance
    -[Pub] approve #
    -[Pub] transferFrom #
    -[Pub] increaseAllowance #

Contract functions details

-[Pub] decreaseAllowance #
-[Int] _transfer #
-[Int] _mint #
-[Int] _burn #
-[Int] _approve #
-[Int] __setupDecimals #
-[Int] _beforeTokenTransfer #

+Ownable (Context)
-[Int] <constructor>
-[Pub] owner
-[Pub] renounceOwnership #
-modifiers: onlyOwner
-[Pub] transferOwnership #
-modifiers: onlyOwner

+GOVI (ERC20, Ownable)
-[Pub] <constructor>

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

- **Critical Severity Issues**
  No critical severity issue found.
- **High Severity Issues**
  No high severity issues found.
- **Medium Severity Issues**
  No medium severity issues found.
- **Low Severity Issues**
  One low severity issue found.

1.Old compiler version

- **Description**
  Contract has been deployed using too old solidity version.
- **Recommendation**
  It is advisable to deploy contract using any of the latest version of solidity.

Centralization

Owner Privileges:

- Owner can transfer and renounce ownership.

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble as smart contract ownership has not been renounced. Following are Admin functions:

- Transferownership
- Renounceownership

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner