



Smart Contract Security Audit Report

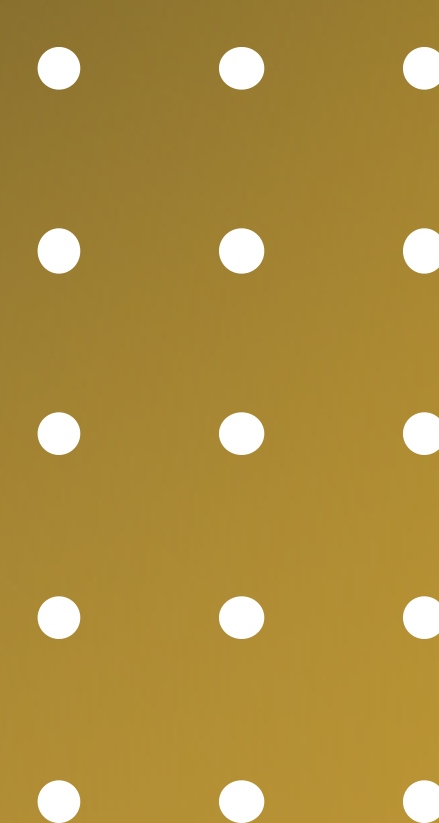
Gnosis

April 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Gnosis



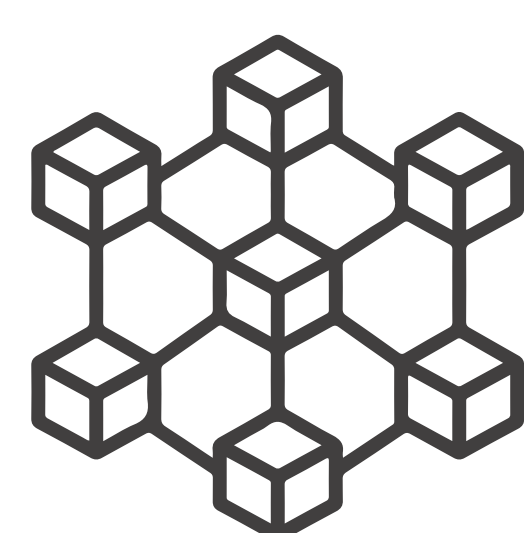
Deployer address

0xbe4e25443Df23382228E6347b06565edD838f901



Client contacts

Gnosis team



Blockchain

Etherscan



Website

<https://gnosis.io/>

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.

Background

HeckSafe was commissioned by Gnosis to perform an audit of smart contracts:

- <https://etherscan.io/address/0x6810e776880c02933d47db1b9fc05908e5386b96#code>

Contract Details

Token contract details for 30.04.2022

Contract name	: GnosisToken
Contract address	: 0x6810e776880C02933D47DB1b9fc05908e5386b96
Total supply	: 10,000,000
Token Ticker	: 10,000,000
Decimals	: 18
Token Holders	: 15,396
Transactions count	: 284,510
Contract deployer address	: 0xbe4e25443Df23382228E6347b06565edD838f901

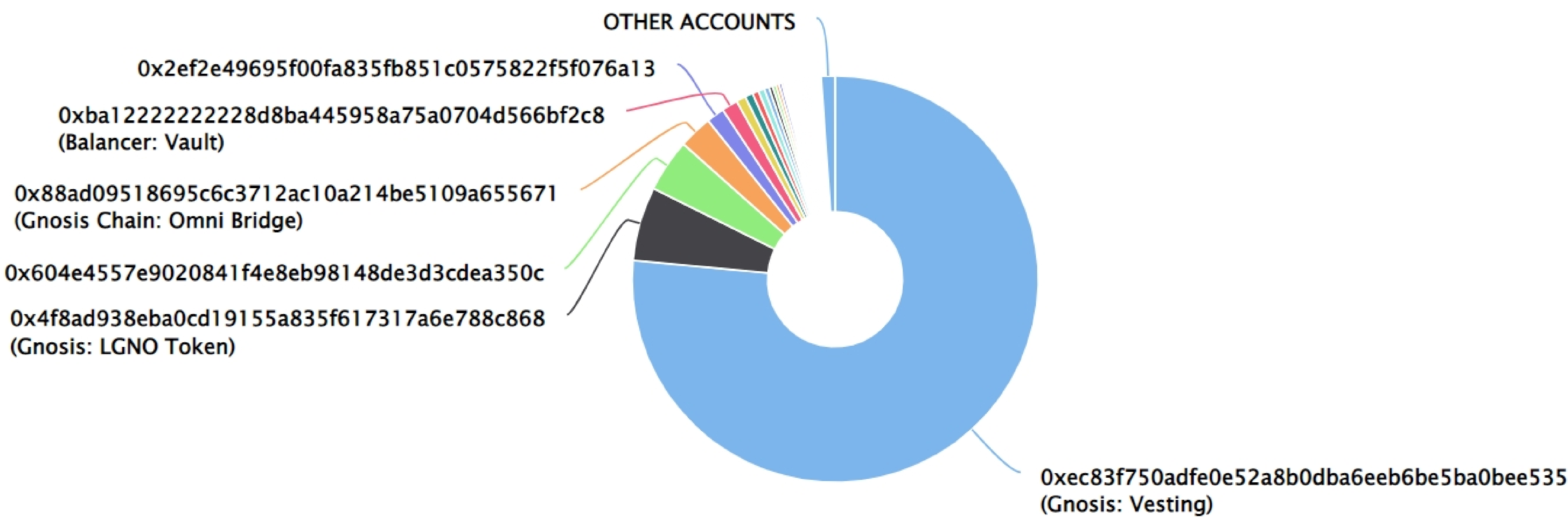
Gnosis Token Distribution

The top 100 holders collectively own 98.89% (9,888,838.47 Tokens) of Gnosis

Token Total Supply: 10,000,000.00 Token | Total Token Holders: 15,397










Gnosis Top 100 Token Holders

Source: Etherscan.io



Gnosis Top 10 Token Holders

(A total of 9,433,457.40 tokens held by the top 10 accounts from the total supply of 10,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 Gnosis: Vesting	7,648,855.998736304185432091	76.4886%
2	 Gnosis: LGNO Token	588,378.354528213878806047	5.8838%
3	 0x604e4557e9020841f4e8eb98148de3d3cdea350c	420,410.999999999999999999	4.2041%
4	 Gnosis Chain: Omni Bridge	266,842.998847909993492997	2.6684%
5	 0x2ef2e49695f00fa835fb851c0575822f5f076a13	144,400.6556	1.4440%
6	 Balancer: Vault	126,948.155516298668608069	1.2695%
7	 Uniswap V3: GNO 2	76,059.362826339587338673	0.7606%
8	 0x5e78c09984bd6608f8e913f0924062c043ed6ad7	61,524.32245887422848027	0.6152%
9	0xa4a6a282a7fc7f939e01d62d884355d79f5046c1	50,251	0.5025%
10	 Gnosis: Active Treasury Management	49,785.555181654364612499	0.4979%

Contract functions details

+ Token

- transfer #
- transferFrom #
- approve #
- totalSupply
- balanceOf
- allowance

+ StandardToken (Token)

- [Pub] transfer #
- [Pub] transferFrom #
- [Pub] approve #
- [Pub] allowance
- [Pub] balanceOf

+ GnosisToken (StandardToken)

- [Pub] GnosisToken #

(\$) = 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

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 issue found.

✔ Medium Severity Issues

No medium severity issues found.

✔ Low Severity Issues

No low severity issue found.

Conclusion

Smart contract contains no 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.