



# Smart Contract Security Audit Report

---

## Spore

May 2022

Security Status



[www.hacksafe.io](https://www.hacksafe.io)



# Audit Details



## Audited project

Spore



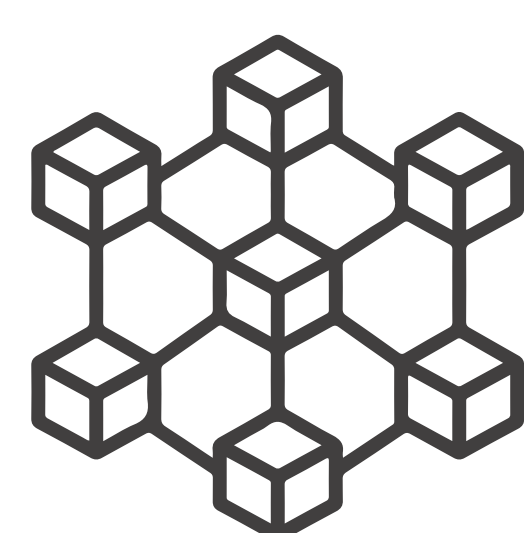
## Deployer address

0x88Dd784dFaaB1a7752d2CC81071Fcd12C1c4E1db



## Client contacts

Spore team



## Blockchain

Avalanche



## Website

<https://spore.earth/>



# 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 spore to perform an audit of smart contracts:**

- <https://snowtrace.io/address/0x6e7f5c0b9f4432716bdd0a77a3601291b9d9e985#code>



# Contract Details

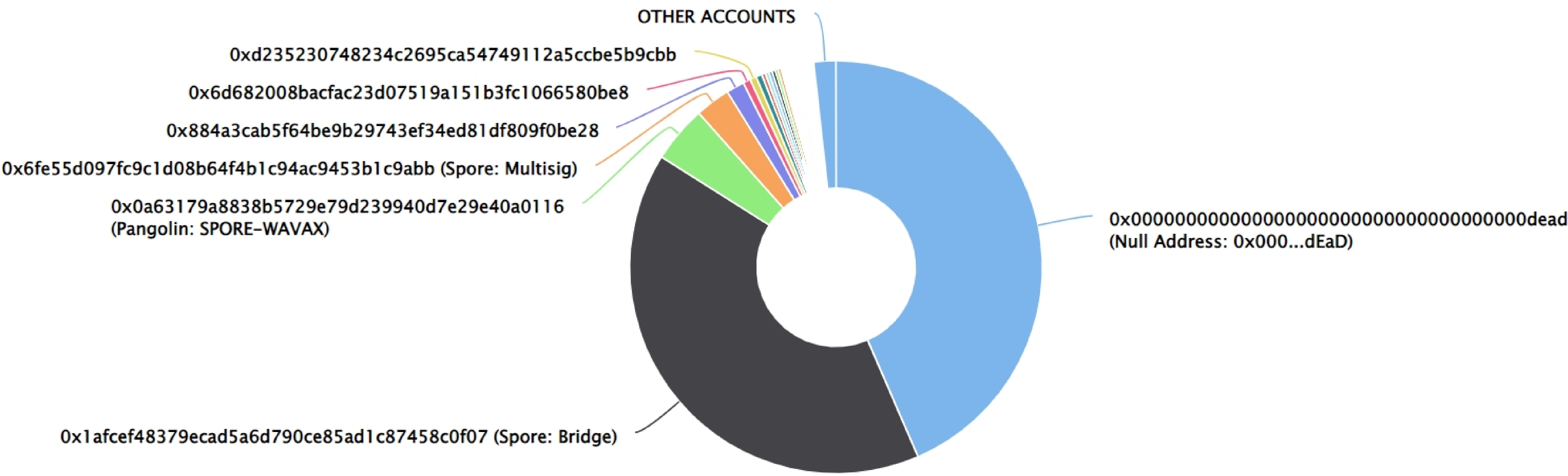
## Token contract details for 10.05.2022

Contract name	: SPORE
Contract address	: 0x6e7f5C0b9f4432716bDd0a77a3601291b9D9e985
Total supply	: 100,000,000,000,000,000
Token Ticker	: SPORE
Decimals	: 9
Network	: SnowTrace
Token Holders	: 6,094
Transactions count	: 55,619
Contract deployer address	: 0x88Dd784dFaaB1a7752d2CC81071Fcd12C1c4E1db
Owner address	: 0x00




# Spore Token Distribution

Spore Top 100 Token Holders

Source: snowtrace.io



## Spore Top 20 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	43,508,000,784,617,200.934312214	43.5080%
2	 Spore: Bridge	40,455,858,208,534,700.140911131	40.4559%
3	 Pangolin: SPORE-WAVAX	4,452,665,258,759,300.073685892	4.4527%
4	 Spore: Multisig	2,758,872,521,161,270.869441107	2.7589%
5	0x884a3cab5f64be9b29743ef34ed81df809f0be28	1,400,976,394,501,400.515735335	1.4010%
6	0x6d682008bacfac23d07519a151b3fc1066580be8	604,207,173,551,968.613926352	0.6042%
7	0xd235230748234c2695ca54749112a5ccbe5b9cbb	501,032,914,724,752.596959009	0.5010%
8	0xf7d5782719690994374ab25f9efa334391770be5	463,814,977,600,762.175432014	0.4638%
9	0xae6d6f831170bb11e8b36bb992cfdffa7d06559a	300,495,434,666,784.598528238	0.3005%
10	0xf30a6e52772335983eb996ff5010ec5d81ace38d	265,783,794,515,807.644565631	0.2658%
11	0x9f3dd31f4fd748f2a73d90cf68529d7518aadfb4	262,511,800,795,235.311905917	0.2625%
12	0xcbe19f73fedd492a10339c431db4eda6ec6eea32	248,468,525,875,267.801992754	0.2485%
13	0x80be2689bcfdf04f4893cb76375e04b2d7d727c9	239,637,832,784,890.969410889	0.2396%
14	0x1576c5bd9bb8717e452a3f46b649cacff5003184	230,115,814,057,393.333013847	0.2301%
15	0x1b12ee9211b3bd417ce9fcc8bfd82b20b2bed21a	138,815,785,815,574.144779574	0.1388%
16	0x246400b96877057479649c46ff21e935c6fe3c7e	123,317,003,533,258.100933808	0.1233%
17	0x0342bf051724c2697362a3b947e170b4bea63299	120,005,412,213,009.53147107	0.1200%
18	0x6720b49d01db2d5b6129ccb73b0f9a752b0cb486	115,880,065,026,369.89640212	0.1159%
19	0xdecd4b961b1984c44afbadbe2844777a627572aa	114,432,486,244,857.153749817	0.1144%
20	0x84a0e780cef0e53315e7c03afee7bbd8c37be3d8	106,570,123,752,752.444221298	0.1066%

# Contract functions details

## + Context

- [int] \_msgsender
- [Int] \_msgData

## + [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer#
- [Ext] allowance
- [Ext] approve#
- [Ext] transferFrom#

## + [Int] IERC20Metadata (IERC20)

- [EXT] name
- [Ext] symbol
- [Ext] decimals

## + [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

## + [Lib] Address

- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Pvt] \_functionCallWithValue



# Contract functions details

+Ownable(Context)

<Constructor>#

-[Pub] owner

-[Pub] renounceOwnership#

-Modifier: onlyOwner

-[Pub] transferOwnership#

-Modifiers: onlyOwner

+SPOR (Context, IERC20, Ownable)

<Constructor>#

- [Pub] name

- [Pub] symbol

- [Pub] decimals

- [Pub] totalsupply

-[Pub] balanceOf

-[Pub] transfer#

-[Pub] allowance

-[Pub] approve#

-[Pub] transferFrom#

-[Pub] increaseAllowance#

-[Pub] decreaseAllowance#

-[Pub] isExcluded

-[Pub] totalFees

-[Pub] reflect#

-[Pub] reflectionFromToken#

-[Pub] tokenFromReflection

-[Ext] excludeAccount#

-[Ext] includeAccount

-[Pvt] \_approve#

-[Ext] enableFairLaunch#

-Modifiers: onlyOwner

-[Pvt] \_transfer#

-[Pvt] \_transferStandard#

-[Pvt] \_\_transferToExcluded #

-[Pvt] \_transferFromExcluded#

-[Pvt] \_transferBothExcluded#

-[Pvt] \_reflectFee #



# Contract functions details

- [Pvt] \_getValues
- [Pvt] \_getTValues
- [Pvt] \_getRValues
- [Pvt] \_getRate
- [Pvt] \_getCurrentSupply

(\$) = payable function

# = non-constant function

# Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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

One low severity issue found.

### 1. Unlocked Compiler Version.

- **Description**

The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version v0.7.6 the contract should contain the following line:

```
pragma solidity 0.7.6;
```

# Owner Privileges

## Owner Privileges (in the period when the owner is not renounced) :

- Spore Contract:
  - Owner can renounce ownership.
  - Owner can transfer ownership.
  - Owner can add or remove account from fees.
  - Owner can add time for trade.

# Conclusion

Smart contract contains low severity issues!

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.