CERTIK

Security Assessment

Sperax

Nov 18th, 2021

Table of Contents

Summary

This report has been prepared for Sperax to discover issues and vulnerabilities in the source code of the Sperax project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Sperax
Platform	Ethereum
Language	Solidity
Codebase	https://etherscan.io/address/0xb4a3b0faf0ab53df58001804dda5bfc6a3d59008#code
Commit	

Audit Summary

Delivery Date	Nov 18, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

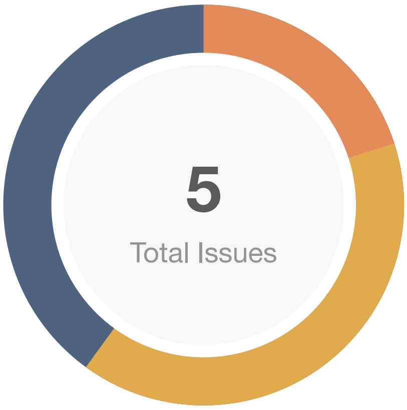
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0
● Major	1	0	0	0	1	0
● Medium	2	0	0	1	0	1
● Minor	0	0	0	0	0	0
● Informational	2	0	0	1	0	1
● Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
SPA	SPA_ERC20_new.sol	ef6dbca19d209378a8c5e21fe9364c2f5db07b47af4a1b8139c570e4344e5b78

Findings



🟥 **Critical**	**0** (0.00%)
🟧 **Major**	**1** (20.00%)
🟨 **Medium**	**2** (40.00%)
Minor	**0** (0.00%)
🟦 **Informational**	**2** (40.00%)
🟩 **Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
SPA-01	Proper Usage of `public` and `external` Type	Gas Optimization	● Informational	ⓘ Acknowledged
SPA-02	Comparison with boolean	Coding Style	● Informational	✓ Resolved
SPA-03	Initial token distribution	Control Flow	● Medium	✓ Resolved
SPA-04	No limit of SPA totalSupply	Logical Issue	● Medium	ⓘ Acknowledged
SPA-05	Centralization Risk on `mintForUSDs`	Logical Issue	● Major	Partially Resolved

SPA-01 | Proper Usage of `public` and `external` Type

Category	Severity	Location	Status
Gas Optimization	● Informational	contracts/Spa/SPA_ERC20_new.sol (Spa): 800~807	ⓘ Acknowledged

Description

`public` functions that are never called by the contract could be declared `external`. When the inputs are arrays `external` functions are more efficient than `public` functions.

Recommendation

The function `batchTransfer()` could be declared `external`.

Alleviation

The team acknowledged the finding, and decided to retain the code base unchanged.

SPA-02 | Comparison with boolean

Category	Severity	Location	Status
Coding Style	● Informational	contracts/Spa/SPA_ERC20_new.sol (Spa): 650	✓ Resolved

Description

Performs comparison with a boolean literal false which can be replaced with the negation of the expression to increase the legibility of the codebase. Moreover, the input parameter `account` lacks a zero-address check.

Recommendation

Consider modifying like below:

```
function setUSDsAddr(address account) onlyOwner external {
    require(!USDsAddrSet, "address already set");
    require(account != address(0), "ERC20: setUSDsAddr to zero address");
    USDsAddr = account;
    USDsAddrSet = true;
}
```

Alleviation

Sperax team removed function `setUSDsAddr` when this contact deployed in address `0xb4a3b0faf0ab53df58001804dda5bfc6a3d59008` of ETH chain.

SPA-03 | Initial token distribution

Category	Severity	Location	Status
Control Flow	● Medium	contracts/Spa/SPA_ERC20_new.sol (Spa): 659	✓ Resolved

Description

All of the `SPA` tokens are sent to the contract deployer when deploying the contract. This could be a centralization risk as the deployer can distribute `SPA` tokens without obtaining the consensus of the community.

Recommendation

We recommend the team to be transparent regarding the initial token distribution process.

Alleviation

[Sperax]: Allocation of `SPA` from the private sale (15% of total supply) has begun under a strict vesting schedule. Vesting for the team and advisors (10% of total supply) vests linearly over 2 years with a 6-month cliff. Foundation funds (25% of total supply) are used to make markets in the early stages and for future protocol development. The SPA treasury will vest linearly over a 4-year time-lock, beginning from the launch date of governance protocol.

The 5 billion `SPA` tokens are distributed as the below list:

- 5% Public sale
- 10% Team & Advisor
- 10% Bootstrap Liquidity
- 10% Staking Rewards
- 15% Private Sale
- 25% Foundation
- 25% Treasury

For more information, please refer to the link: https://medium.com/sperax/sperax-multi-sig-the-road-to-decentralization-3044ea841836

Since the below-listed reasons, the development team thinks it is necessary to mint the new `SPA` token after deployment:

1. `USDs` stable-coin protocol, the flagship product of Sperax, requires the minting function of SPA. The economic system of USDs is a dual-token system of USDs and SPA. Especially, it means that when the user redeems USDs, the new SPA must be minted so that the user can always obtain a one-dollar-worth package of tokens. Hence, in order for `USDs` stable-coin protocol to work properly, SPA must be elastic. In other words, SPA must have the minting function. For the details of the dual-token system of USDs, please check section 2 of the `USDs` whitepaper.
2. SPA Arbitrum custom cross-chain gateway requires the minting function of SPA. Since USDs is launched on Arbitrum Layer-2, SPA resides on both Arbitrum Layer-2 and Ethereum Layer-1. The `USDs` protocol requires that the SPA cross-chain gateway must adopt a custom gateway. This custom gateway, in turn, requires that SPA must be elastic on Layer-1. In other words, SPA must have the minting function.

SPA-04 | No limit of SPA totalSupply

Category	Severity	Location	Status
Logical Issue	● Medium	contracts/Spa/SPA_ERC20_new.sol (Spa)	ⓘ Acknowledged

Description

There is no limit of the tokens totalSupply.

Recommendation

We recommend that the team limit the totalSupply of `SPA` tokens

Alleviation

The team responded that this is the intention of the design.

SPA-05 | Centralization Risk on `mintForUSDs`

Category	Severity	Location	Status
Logical Issue	● Major	contracts/Spa/SPA_ERC20_new.sol (Spa): 691~693	Partially Resolved

Description

The function `mintForUSDs()` is merely called by the user in `mintableGroup`, and it allows the caller to mint any amount of tokens to any specified recipient. To improve the trustworthiness of this protocol, any plan to the mint token is better to move to the execution queue of `Timelock` and also add an `emit event`, or make the owner Multi-sig.

```
691   function mintForUSDs(address account, uint256 amount) whenMintNotPaused
onlyMintableGroup external {
692       _mint(account, amount);
693   }
```

Recommendation

We advise the client to carefully manage the `mintableGroup` account's private key to avoid any potential risks of being hacked.

In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

Currently, Sperax token is deployed at address `0xB4A3B0Faf0Ab53df58001804DdA5Bfc6a3D59008` on ETH.

The owner of this contract is a multi-sig `GnosisSafeProxy` contract at address `0x86c87113dc3497361b7c5bad66d67303ddf4611f`, and the implementation of this proxy is deployed at address `0xd9db270c1b5e3bd161e8c8503c55ceabee709552`.

Now there are below three owner addresses manage this multisig contract:

1. 0xc28c6970d8a345988e8335b1c229dea3c802e0a6
2. 0x42d2f9f84eeb86574aa4e9fcccfd74066d809600
3. 0x4f987b24bd2194a574bb3f57b4e66b7f7ed36196

[Sperax]: Next Steps Towards Decentralization

1. Move funds to wallets managed by multi-sig
2. Add time lock based on the proposed vesting schedule
3. Add protocol upgrade delay
4. Burn admin keys and transfer ownership to governance contracts

Refer to the official announcement about decentralization: https://medium.com/sperax/sperax-multi-sig-the-road-to-decentralization-3044ea841836

Appendix

Finding Categories

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we’re able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

CERTIK