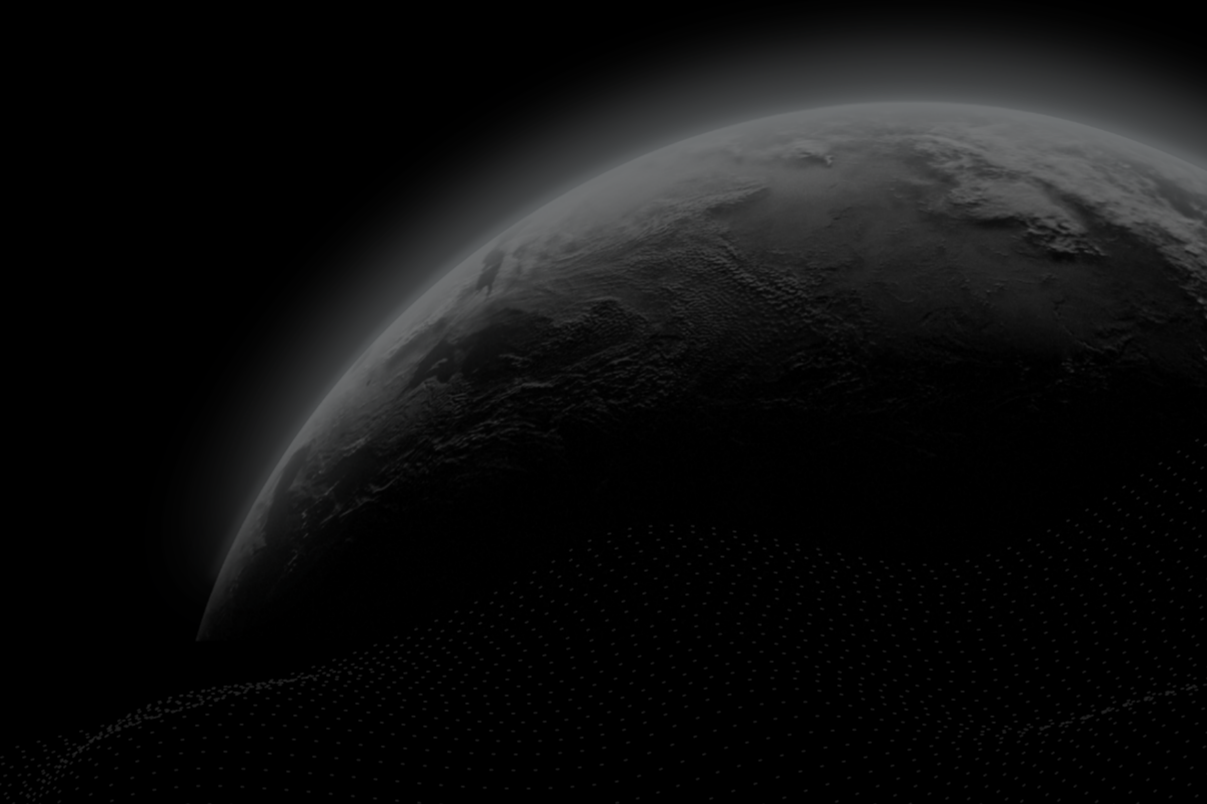
Security Assessment

STYLE Protocol

CertiK Verified on Mar 27th, 2023



CertiK Verified on Mar 27th, 2023

STYLE Protocol

The security assessment was prepared by CertiK, the leader in Web3.0 security.

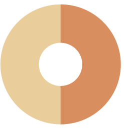
Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Ethereum (ETH)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 03/27/2023	N/A

CODEBASE	COMMITS
0xa962fc9d092c1e2de00bf600e261cf058b5685b1 ...View All	0xa962fc9d092c1e2de00bf600e261cf058b5685b1 ...View All

Vulnerability Summary



2	1	1	0	0	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

🟥	0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
🟧	1	Major	1 Mitigated	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
🟨	0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨	1	Minor	1 Resolved	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
🟦	0	Informational		Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | STYLE PROTOCOL

CODEBASE | STYLE PROTOCOL

Repository

0xa962fc9d092c1e2de00bf600e261cf058b5685b1

Commit

0xa962fc9d092c1e2de00bf600e261cf058b5685b1

AUDIT SCOPE | STYLE PROTOCOL

9 files audited ● 1 file with Mitigated findings ● 8 files without findings

ID	File	SHA256 Checksum
● SOU	Source.sol	be32a577155d99c4bf15092bd2eab9dc86fe089a0c1d586f99a8083c1a74f8f2
● ADD	Address.sol	4ee17cf59421e94005916b4ca3ccd7b90af3a95298dc4fde0914aa9bdff74c3f
● CON	Context.sol	6ee66d1e4693ec63d29393cc2c83594798475ad0eeabcb0951a35780ef003113
● ERC	ERC777.sol	a9f0ee091108bc2f6e64bb75cc70f047a1594604bff38e54cd7b8d2e711e2854
● IER	IERC1820Registry.sol	4c722d4460537f5b55d35a4d78d50e15c1bdc6bf1c0af87086bc71ae69eccfbb
● IEC	IERC20.sol	9be043cb9394f0fdfd7bfa0ae9201bedb08ce930a3da8c2c5cfdae56ae7eb13f
● IRC	IERC777.sol	3bdaec860d7c203c3912f602ae615df61e009f70c109a28f23e6f7f70d4c36fe
● IRR	IERC777Recipient.sol	0942ea1b056fb9af87f5f81d7f68249398a6eb4c7bbf7eaf74aef5f4da8f8652
● IES	IERC777Sender.sol	8172fca5a40bdfb550e90f84efeabbd9d706235998c881978f7bff5b566fb7b4

APPROACH & METHODS | STYLE PROTOCOL

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

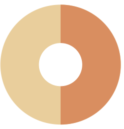
The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

REVIEW NOTES | STYLE PROTOCOL

The `Style Protocol` project audited within this report is an ERC777 token contract which has already been launched to Ethereum mainnet (see the codebase link). This project is a fork of OpenZeppelin's ERC777 code, the only notable difference being an initial minting of 920,000,000 `STYLE` tokens to the `msg.sender` deploying the contract this address is described on-chain as STYLE Protocol: Deployer. This initial distribution can be seen in transaction hash 0x8d84590a1787c106a593722c5879ca7879700e9fc325a2498058a6ea50efdf7e.

FINDINGS | STYLE PROTOCOL



2	0	1	0	1	0
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for STYLE Protocol. Through this audit, we have uncovered 2 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
SOU-01	**Initial Token Distribution**	**Centralization / Privilege**	**Major**	● **Mitigated**
SOU-02	Missing Input Validation	Volatile Code	Minor	● Resolved

SOU-01 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**Source.sol: 15**	● **Mitigated**

Description

All `STYLE` tokens are sent to the contract deployer when deploying the contract. This is a potential centralization risk as the deployer can distribute `STYLE` tokens without the consensus of the community.

Recommendation

We recommend transparency through providing a breakdown of the intended initial token distribution in a public location, such as public medium article, or public project documentation on the project website. We also recommend the team make an effort to restrict the access of the corresponding private key.

Alleviation

`[CertiK]` : 2023/02/22 - 16:43 UTC - blockheight 16684942 :
Currently 98.4144% of the total supply is in the gnosis safe at address: 0x093a6b4b812478e9603f5c140e09d0e949f5a7be, there are two owners:

1. STYLE Protocol: Deployer which is an externally owned account.
2. 0xe1Dd668d7685Ed339d9315110d7e1007c37FE318

Please see the team's whitepaper (Version 1.2.0) **here** for an outline of their token distribution plans:

- Protocol (= 38%)
  - Team = 12% (Linear Vesting over 48 months to ensure slow distribution.)
  - Investors = 22% (Linear Vesting over 36 months to ensure slow distribution.)
  - Advisors = 4% (Linear Vesting over 18 months to ensure slow distribution.)
- Community / Later DAO (=62%)
  - Initial Launch: Given to public via CEX = 42% (Sold publicly at launch for anyone to participate.)
  - Ecosystem Growth = 10% (Long Term) (Locked first and then vested over 36 months to be invested strategically in growth and offered for funding of ecosystem projects.)
  - Community Development = 10% (Long Term) (Initial and then vested over 60 months to be invested in long-term community building and growth of participants.)

SOU-02 | MISSING INPUT VALIDATION

Category	Severity	Location	Status
Volatile Code	● Minor	Source.sol: 10	● Resolved

Description

The constructor of the `styleToken` contract is missing a check that `initialSupply > 0`.

Recommendation

We recommend adding a check the passed-in uint is not zero to prevent unexpected errors.

Alleviation

`[CertiK]`: This contract is deployed at address 0xa962fc9d092c1e2de00bf600e261cf058b5685b1 with 920,000,000 `STYLE` tokens minted as the initial supply at transaction hash 0x8d84590a1787c106a593722c5879ca7879700e9fc325a2498058a6ea50efdf7e, so this instance has a non-zero amount of tokens.

APPENDIX | STYLE PROTOCOL

Finding Categories

Categories	Description
Centralization / Privilege	Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

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 | CERTIK

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.

CertiK | **Securing** the **Web3** World

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.