CERTIK

Security Assessment

SmartAlpha

Aug 4th, 2021

Table of Contents

Summary

This report has been prepared for BARNBRIDGE to discover issues and vulnerabilities in the source code of the SmartAlpha 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 only minor and informational findings. We recommend addressing these findings to ensure a high level of security standards and industry practices.

Overview

Project Summary

Project Name	SmartAlpha
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/BarnBridge/SmartAlpha
Commit	29679c3d595444e79f78a39ceeca9918e4d009d1 6d045e3656518f61934e57105aabfa501731a977

Audit Summary

Delivery Date	Aug 04, 2021
Audit Methodology	Manual Review, Static Analysis
Key Components	

Vulnerability Summary

Vulnerability Level	Total	Pending	Partially Resolved	Resolved	Acknowledged	Declined
● Critical	0	0	0	0	0	0
● Major	0	0	0	0	0	0
● Medium	0	0	0	0	0	0
● Minor	5	0	3	2	0	0
● Informational	1	0	0	1	0	0
● Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
AVI	interfaces/AggregatorV3Interface.sol	8d613530b3ef890f492c2fce056d7792cdeb194d1498321e52ccee1086a175fe
IAM	interfaces/IAccountingModel.sol	410dd5a2f8ca44755ed74bbc5fc57656c4fc6596b16a0a6cb0348cd8c3ee6b83
IOE	interfaces/IOwnableERC20.sol	42f7861e244d2b35293cb77eefcc7700fcf523111f7aec6fc647ed1d97081057
IPO	interfaces/IPriceOracle.sol	d07f7d32b69f7f92a7dac4bba91306876f4d74f1262b7acb445994b96e0ae898
ISR	interfaces/ISeniorRateModel.sol	79214d29a7009b27b919cef5068fa096417dc8bceb7eccc964007e74af653435
AMS	AccountingModel.sol	9cd55b63112f5a820355a1f1e70f83bf3c9d3c576557774d40bc1a02739951d2
COS	ChainlinkOracle.sol	d4ffa347671cf5ab17f7162653c705ad1c12bc0466a968bd3327fe24bafef086
GSA	Governed.sol	d6fa0aca269cdbb857733575e3424588c6a3d96f702d5366ae691fa4f6759d3a
OER	OwnableERC20.sol	a9749355bb04e00c3b3aaeb18e056ee1b2b9788ed086c974b2aceb3a332a1a94
SRM	SeniorRateModel.sol	c65d8aae65ed7e493c9d92da61be93c17e269cce468d37120fb4e909809b51eb
SAA	SmartAlpha.sol	7e8709e7456c42c9b252a285db3f95b84ca59691b20c3b5ffde5638072c1c590
SAE	SmartAlphaEvents.sol	8574bc3bd8dd39929068e8f903ad66ed2580d35e6e1fe5ae167ab62df338b476

There are a few depending injection contracts or addresses in the current project:

- `poolToken`, `juniorToken`, and `seniorToken` for contract `SmartAlpha`;
- `priceOracle`, `seniorRateModel` and `accountingModel` for contract `Governed`;
- `oracle` for contract `ChainlinkOracle`.

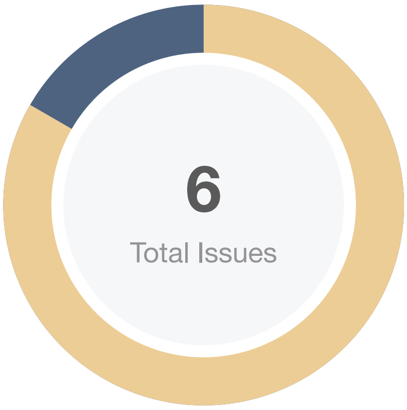
We assume these contracts or addresses are valid and non-vulnerable actors and implementing proper logic to collaborate with the current project.

To set up the project correctly, improve overall project quality and preserve upgradability, the following roles, are adopted in the codebase:

- `dao`, is adopted to initialize the contract `SmartAlpha` in contract `SmartAlpha`;
- `dao`, is adopted to update the value of sensitive variables `dao`, `priceOracle`, `seniorRateModel`, `accountingModel`, `feesOwner`, and `feesPecentage` in contract `Governed`;
- `guardian`, is adopted to update transfer the guardianship, pause and unpause the whole contract in contract `Governed`;
- `owner`, is adopted to mint, burn and transfer tokens in contract `OwnableERC20`.

To improve the trustworthiness of the project, dynamic runtime updates in the project should be notified to the community. Any plan to invoke the aforementioned functions should be also considered to move to the execution queue of the `Timelock` contract.

Findings



🟥	**Critical**	**0** (0.00%)
🟧	**Major**	**0** (0.00%)
🟨	**Medium**	**0** (0.00%)
🟨	**Minor**	**5** (83.33%)
🟦	**Informational**	**1** (16.67%)
🟩	**Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
GSA-01	Centralization Risk	**Centralization / Privilege**	● **Minor**	**Partially Resolved**
OER-01	Centralization Risk	**Centralization / Privilege**	● **Minor**	**Partially Resolved**
SAA-01	Check-Effect-Interaction Pattern Violation	Logical Issue	● Minor	✓ Resolved
SAA-02	Lack of Return Value Handling	Logical Issue	● Minor	✓ Resolved
SAA-03	Centralization Risk	**Centralization / Privilege**	● **Minor**	**Partially Resolved**
SAA-04	Unused Import File	Coding Style	● Informational	✓ Resolved

GSA-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Minor	Governed.sol: 38, 52, 64, 75, 75, 87, 99, 111, 123, 135, 135	Partially Resolved

Description

In the contract `Governed`, the role `dao` has the authority over the following functions:

- `Governed.transferDAO()`: Update `dao`.
- `Governed.setPriceOracle()`: Update `priceOracle`.
- `Governed.setSeniorRateModel()`: Update `seniorRateModel`.
- `Governed.setAccountingModel()`: Update `accountingModel`.
- `Governed.setFeesOwner()`: Update `feesOwner`.
- `Governed.setFeesPercentage()`: Update `feesPercentage`.
- `Governed.transferGuardian()`: Update the address of `guardian`.
- `Governed.pauseSystem()`: Pause the whole contract.
- `Governed.resumeSystem()`: Resume the whole contract.

The role `Guardian` has the authority over the following functions:

- `Governed.transferGuardian()`: Update the address of `guardian`.
- `Governed.pauseSystem()`: Pause the whole contract.
- `Governed.resumeSystem()`: Resume the whole contract.

Any compromise to the `dao` or `guardian` account may allow the hacker to manipulate the project through these functions.

Recommendation

We advise the client to carefully manage the `dao` and `guardian` accounts' private keys if they are EOAs 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

[**BarnBridge**]: The DAO is a contract governed by the community. The Guardian has limited power and will be a MultiSig.

OER-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Minor	OwnableERC20.sol: 17, 27, 38	Partially Resolved

Description

In the contract `OwnableERC20`, the role `owner` has the authority over the following function:

- `OwnableERC20.mint()`: Mint a number of tokens to the address `user`.
- `OwnableERC20.burn()`: Burn a number of tokens belonging to the address `user`.
- `OwnableERC20.transferAsOwner()`: Transfer a number of tokens from the address `sender` to the address `recipient`.

Recommendation

We advise the client to carefully manage the `owner` account's private key if it is an EOA 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

[**BarnBridge**]: Contract `SmartAlpha` enforces that the junior and senior tokens which will use the OwnableERC20 contract are owned by the contract itself or reverts the initialization. Only the users through their actions can trigger the privileged functions on the OwnableERC20, which is as decentralized as it can be.

[**CertiK**]: We came up with this issue because we assume the contract is not only used in the contract `SmartAlpha`.

We agree that there is not centralization risk when the contract `OwableERC20` is used in the contract `SmartAlpha`.

SAA-01 | Check-Effect-Interaction Pattern Violation

Category	Severity	Location	Status
Logical Issue	● Minor	SmartAlpha.sol: 167, 201, 224, 254, 114, 307, 362, 385	✓ Resolved

Description

The Solidity documentation suggests that a smart contract should follow the `Checks-Effects-Interactions` pattern. However, the functions at the aforementioned lines violate the `Checks-Effects-Interactions` pattern by having external calls (Interactions) before event emissions (Effects).

Recommendation

We recommend adopting the `Checks-Effects-Interactions` pattern in the aforementioned functions by, for example, emitting events before processing external calls.

Alleviation

[**BarnBridge Team**]: After reviewing the reported functions, we concluded that most of them are false positives. We only interact with trusted tokens.

[**CertiK**]: We came up with this issue because we did not assume external dependencies can be trusted.

However, we agree that if the tokens used within the contract are all trusted then this will not be an issue.

SAA-02 | Lack of Return Value Handling

Category	Severity	Location	Status
Logical Issue	● Minor	SmartAlpha.sol: 215, 268, 298, 353	✓ Resolved

Description

The following functions are not void-returning functions:

- `juniorToken.transfer()`
- `seniorToken.transfer()`
- `juniorToken.transferAsOwner()`
- `seniorToken.transferAsOwner()`

Ignoring their return values, especially when they represent execution results, might cause unexpected exceptions.

Recommendation

We recommend checking the output of the aforementioned functions before continuing processing.

Alleviation

[**BarnBridge**]: These function calls always return true so checks are unnecessary.

[**CertiK**]: We came up with this issue because the addresses of `juniorToken` and `seniorToken` are set in the function `SmartAlpha.initialize()`, and we only assume the function signatures of these two token contracts are the same as that in `OwnableERC20` while their implementation is non-guaranteed.

However, if `juniorToken` and `seniorToken` are implemented by the contract `OwnerableERC20`, these functions always return true, then handling the return values are not necessary.

SAA-03 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● **Minor**	SmartAlpha.sol: 75	**Partially Resolved**

Description

In the contract `SmartAlpha`, the role `dao` has the authority over the function `SmartAlpha.initialize()` to initialize the contract.

Any compromise to the `dao` account may allow the hacker to manipulate the project through these functions.

Recommendation

We advise the client to carefully manage the `dao` account's private key if it is an EOA 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

[**BarnBridge**]: The DAO is a contract governed by the community.

SAA-04 | Unused Import File

Category	Severity	Location	Status
Coding Style	● Informational	SmartAlpha.sol: 8	✓ Resolved

Description

`hardhat/console.sol` is imported but is never used.

Recommendation

We recommend removing the unused import `hardhat/console.sol` .

Alleviation

The client heeded our advice and fix this issue by deleting unused import in the commit `6d045e3656518f61934e57105aabfa501731a977`.

Appendix

Finding Categories

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.

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.

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