CERTIK

Security Assessment

Hillstone Finance Token

Jun 28th, 2021

Table of Contents

Summary

This report has been prepared for Token smart contracts, to discover issues and vulnerabilities in the source code of their Smart Contract 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 informational findings. 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 given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Hillstone Finance Token
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/Hillstone-Finance/hillstone-finance
Commit	a61775731d9386cd4c0505fc1f2cbe4cd22b395e

Audit Summary

Delivery Date	Jun 28, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

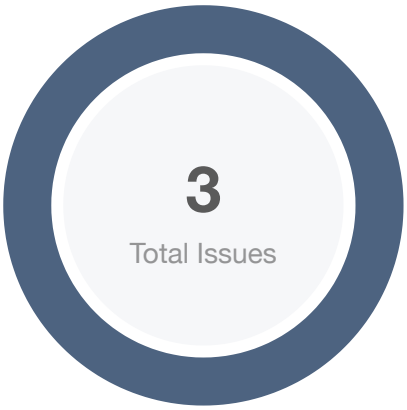
Vulnerability Summary

Vulnerability Level	Total Count	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	0	0	0	0	0	0
Informational	3	0	0	0	3	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	file	SHA256 Checksum
HHF	contracts/HillstoneFinance.sol	e2f6dad2cce7206cccdafaef2e3815596a9efc47711ee2aba423edf0d27983d5

Findings



Critical	**0** (0.00%)
Major	**0** (0.00%)
Medium	**0** (0.00%)
Minor	**0** (0.00%)
Informational	**3** (100.00%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
HFH-01	Uses Literals With Too Many Digits	Coding Style	Informational	Acknowledged
HFH-02	Owner Owns All Tokens	**Centralization / Privilege**	**Informational**	**Acknowledged**
HFH-03	Unlocked Compiler Version	Language Specific	Informational	Acknowledged

HFH-01 | Uses Literals With Too Many Digits

Category	Severity	Location	Status
Coding Style	Informational	contracts/HillstoneFinance.sol: 37	Acknowledged

Description

The linked code represents a value with too many digits making it hard to read.

Recommendation

Consider refactoring the code and using a more explanatory way to represent the value.

Alleviation

The team acknowledged the issue and opted not to alleviate it in the current iteration.

HFH-02 | Owner Owns All Tokens

Category	Severity	Location	Status
Centralization / Privilege	**Informational**	contracts/HillstoneFinance.sol: 40	**Acknowledged**

Description

The owner of the project mints all tokens to his account(to distribute).

Recommendation

Considering providing the rationale in a comment.

Alleviation

The team acknowledged the issue as part of the system.

HFH-03 | Unlocked Compiler Version

Category	Severity	Location	Status
Language Specific	Informational	contracts/HillstoneFinance.sol: 3	Acknowledged

Description

The contract has unlocked compiler version. An unlocked compiler version in the source code of the contract 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 an ambiguity when debugging as compiler specific bugs may occur in the codebase that would be hard to identify over a span of multiple compiler versions rather than a specific one.

Recommendation

We advise that the compiler version is instead locked at the lowest version possible that the contract can be compiled at.

Alleviation

The team acknowledged the issue and opted not to alleviate it in the current iteration.

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.

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.

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 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 without CertiK's prior written consent.

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.

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.