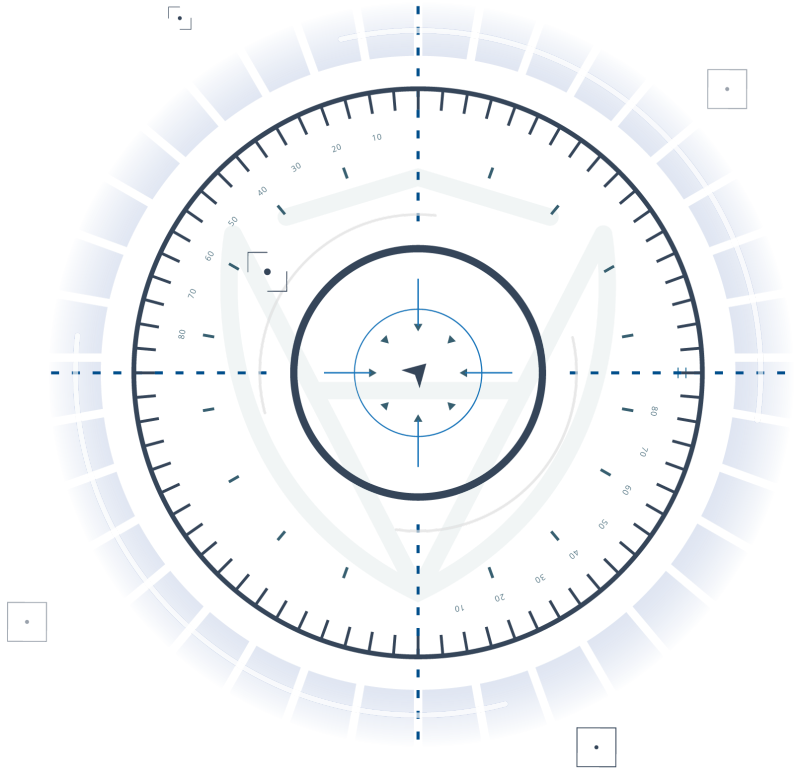
CERTIK

GFC-NFT-LP Protocol

Skynet Scanning Report

May 6th, 2021



Summary

This report is based on the results from CertiK Skynet Scanning, a proprietary security service that leverages automated scanning technologies to check smart contracts against a wide range of known vulnerabilities. Clients could reference the content to reason about the security score calculations. Automated static analysis can cover a wide range of known security issues and vulnerabilities, yet a full security assessment by security experts is always recommended to cover potential security concerns at business levels.

Scope of Works

The nature of CertiK Skynet is to provide real-time security intelligence, and scanning based on static analysis tool sets is one of the 6 Security Primitives. In summary:

1. Smart contracts run against CertiK's in-house tool chains (together with open source libraries for cross-checking purposes);
2. Manual efforts involved in reviewing the scanning outputs and filter out false alarms. We map scanning results into SWCs for better categorizing and we encourage the development team of the projects to visit the website and follow the recommendations: https://swc-registry.certik.foundation/;
3. Manual efforts on a high level walkthrough of code logics to better understand the project and its intentions that may benefit a future full security assessment.

Overview

Below is the very basic manual understanding of the contracts covered by the Skynet Scanning technologies, and none of the contents matter to the final outputs of the software we use. Please refer to the full assessment (if any) for the complete understanding or the walkthroughs of the smart contracts in scope.

LpPool

The contract LpPool takes three tokens, `lp`, `gfv` and `nft`, where `lp` and `gfv` are ERC20 tokens and `nft` is an ERC721 token. The pool can receive `lp` and `nft` and let users take part in rounds of awards.

Scanning Results

Primitive Scores

Source-code Score | 89

- LpPool | 89

Smart Contracts

- LpPool

Source-code Primitive Results

In summary, 5 issues were found out of 33 checks for **LpPool**.

SWC-107	-5 pts
Title	Reentrancy
Contract	LpPool
Location	Line#693-697, 704-710

SWC-115	-3 pts
Title	Authorization through `tx.origin`
Contract	LpPool
Location	Line#13

SWC-CTK-67	-1 pts

Title	Weak Randomness
Contract	LpPool
Location	Line#800

SWC-CTK-44	**-1 pts**
Title	Uninitialized Local Variables
Contract	LpPool
Location	Line#771, 785

SWC-120	**-1 pts**
Title	Block Timestamps
Contract	LpPool
Location	Line#667, 669, 787

Disclaimer

Skynet Scanning could be leveraged as an automated toolset, however, it cannot replace a formal full security assessment, the toolset is best used synergistically alongside a full formal security audit. Security experts are extremely important in analyzing complex business logic and unknown vulnerabilities specific to each organization. QuickScan is a proprietary CertiK service, offered exclusively to existing and potential clients.

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/verification, 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.

About CertiK

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

Provable Trust For All