July 15th, 2022

NuriFlex World PTE., LTD.
SECURITY ASSESSMENT REPORT

version 1.1

General Analysis and Compiler Audit

Audited by SOOHO

SOOHO

Contents

1. Introduction 3

1.1 Disclaimer 3

1.2 Methodology 4

2. Assessment Results 5

2.1 Analysis Target 5

2.2 Summary 6

2.3 Findings 8

2.4 Conclusion 11

About SOOHO 12

1. Introduction

As a beginning, we provide disclaimer and describe how SOOHO audit team approaches VictoryGem Smart Contract methodologically during the security assessment period.

1.1 Disclaimer

• This document is based on a security assessment conducted by a blockchain security company SOOHO. This document describes the detected security vulnerabilities and also discusses the code quality and code license violations.

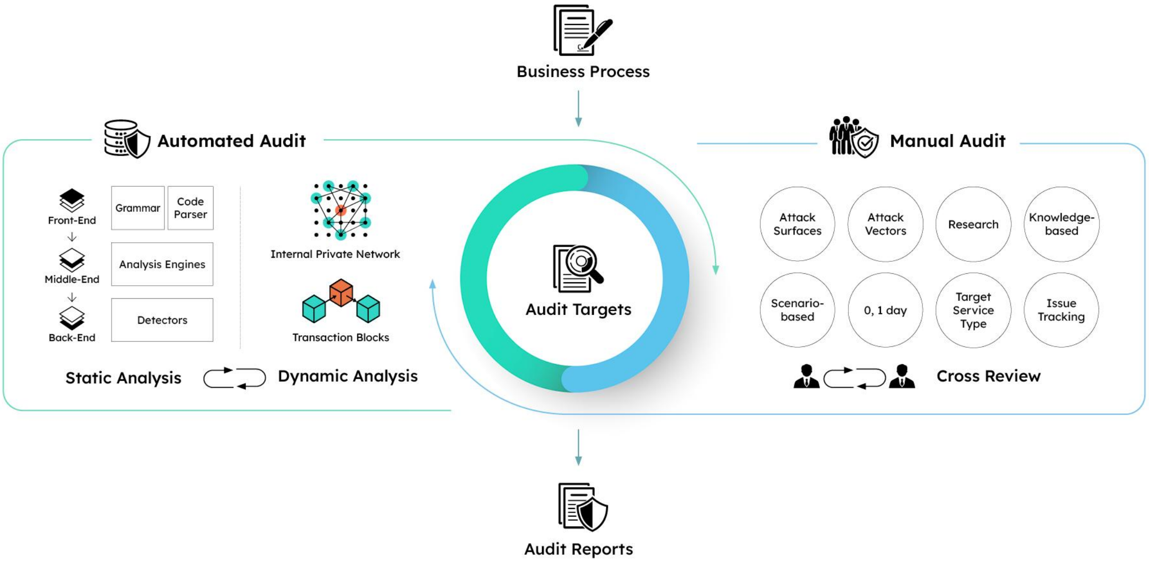
• This security assessment does not guarantee nor describe the usefulness of the code, the stability of the code, the suitability of the business model, the legal regulation of the business, the suitability of the contract, and the bug-free status. Audit document is used for discussion purposes only.

• SOOHO does not disclose any business information obtained during the review or save it through a separate media.

• SOOHO presents its best endeavors in smart contract security assessment.

1.2 Methodology

SOOHO conducts a more complete, continuous blockchain security assessment by applying two audit methodologies: Automated Audit and Manual Audit.



Automated audit ensures high quality of security assessment by finding various attacks quickly and precisely through cooperative analysis between static and dynamic analysis. Our static analyzer analyzes target codes through parsing grammar and verifies constraints through path finding and variable tracking. In dynamic analysis, emulation of target codes is executed in SOOHO's own test network along with fuzzing and concolic execution.

During the manual auditing process, our security experts verify the contract using various security and domain knowledge. Experts preferentially analyze codes with greater risk, check whether the codes are written under the client's intention and supervise access control management. Experts are complementing automated analysis by dealing with complex attack scenarios and recent security issues. We also provide more upgraded security audit reports through cross-review between security experts.

By conducting risk verification using various methodologies as above, SOOHO secures partners' contracts from 1-day to 0-day vulnerabilities.

Detected vulnerabilities are listed on the basis of the risk rating of vulnerability. The risk rating of vulnerability is set based on OWASP's impact & Likelihood Risk Rating Methodology. Some issues were rated vulnerable aside from the corresponding model and the reasons are explained in the following results.

2. Assessment Results

In this section, we describe the overall structure of NuriFlex Smart Contract and provide the summary of findings. Details of detected vulnerabilities are given for improvement in the implementation of NuriFlex Smart Contract.

2.1 Analysis Target

Project	nuriflex-token
# of Files	1
# of Target	1
# of Lines	537
File Tree	nuriflex-token └── NuriFlex.sol

2.2 Summary

Severity	# of Findings
Critical	
High	
Medium	
Low	
Note	■

#	Description	Severity	Status
SH-001	Possible gas optimization by removing SafeMath library	Note	Acknowledged

Key Audit Points

NuriFlex contract is a BEP20 token developed by NuriFlex World PTE., LTD. Accordingly, we mainly reviewed common vulnerabilities in the token specification and gas optimization.

However, we did not take any internal hackings by administrators into account. Analyzes are about the functioning of the subject contract, given the safety of the system.

2.3 Findings

Note Possible gas optimization by removing SafeMath library

File Name	NuriFlex.sol
File Location	NuriFlex.sol
SHA1	a84a282551893844a4d20b2ae58df43b861093f0

Details

In Solidity version 0.8.0 and later, its semantics guarantees that the arithmetic overflow/underflow vulnerability is no longer present. Therefore, the use of SafeMath libraries to block arithmetic overflow/underflow vulnerabilities increases code size and the number of instructions executed each time, resulting in a waste of gas fees.

Mitigation

It is recommended to specify the Solidity version to 0.8.0 or later (the current latest version is 0.8.15) and stop using SafeMath library to reduce gas waste.

Update

NuriFlex team updated Solidity version to 0.8.15. However, since the SafeMath library has not been removed, the gas optimization issue remains.

✔ (Verified) BEP20 Specification

Details

We have confirmed that the NuriFlex contract followed the BEP20 specification with the proper name, symbol, and decimal.

✔ (Verified) SWC-100

Details

We have confirmed that the function visibility is properly developed.

✔ (Verified) SWC-101

Details

We have confirmed that the arithmetic operations are safe.

✓ (Verified) SWC-104

Details

We have confirmed that the argument is properly validated.

✓ (Verified) SWC-107

Details

We have confirmed that the reentrancy vulnerability will not work.

✓ (Verified) SWC-108

Details

We have confirmed that the contract is well architected.

✓ (Verified) SWC-113

Details

We have confirmed that the DoS will not work.

✓ (Verified) SWC-118

Details

We have confirmed that the constructor is well developed.

2.4 Conclusion

The source code of the NuriFlex contract developed by NuriFlex World PTE., LTD. is easy to read and very well organized. We have to remark that contracts are well architected and all the additional features are implemented.

As a result of the code review, there is **1 issue (1 Note)**. We recommend that you stabilize your contract and analyze potential vulnerabilities through a steady code audit.

About SOOHO

SOOHO with the motto of “Audit Everything, Automatically” researches and provides technology for a reliable blockchain ecosystem. SOOHO verifies vulnerabilities through the entire development life-cycle with a vulnerability analyzer created by SOOHO, and open source analyzers.
SOOHO is composed of experts including Ph.D researchers in the field of automated security tools and white-hackers verifying contract codes and detected vulnerabilities in depth. Professional experts in SOOHO secure partners’ contracts from 1-day to 0-day vulnerabilities.

Contact us :)

Twitter:	SOOHO_AUDIT
E-mail:	audit@sooho.io
Website:	https://audit.sooho.io/