July 15th, 2022

NuriFlex World PTE., LTD. SECURITY ASSESSMENT REPORT

version 1.1
General Analysis and Compiler Audit

Audited by SOOHO

SOOHO

목차

1. 개요

‘개요’ 파트에서는 SOOHO 보안 감사 프로세스와 보안 감사에 사용된 방법론을 서술합니다. 분석 내용을 이해하시는 데에 참고하시길 바랍니다.

1.1 시작하기 전에

• 본 문서는 블록체인 보안 전문업체 SOOHO에서 진행한 취약점 검사를 바탕으로 작성한 문서로, 스마트 컨트랙트의 보안 취약점의 발견에 초점을 두고 있습니다. 추가적으로 코드 퀄리티 및 코드 라이센스 위반 사항 등에 대해서도 논의합니다.

• 본 문서는 코드의 유용성, 코드의 안정성, 비즈니스 모델의 적합성, 비즈니스의 법적인 규제, 계약의 적합성, 버그 없는 상태에 대해 보장하거나 서술하지 않습니다. 감사 문서는 논의 목적으로만 사용됩니다.

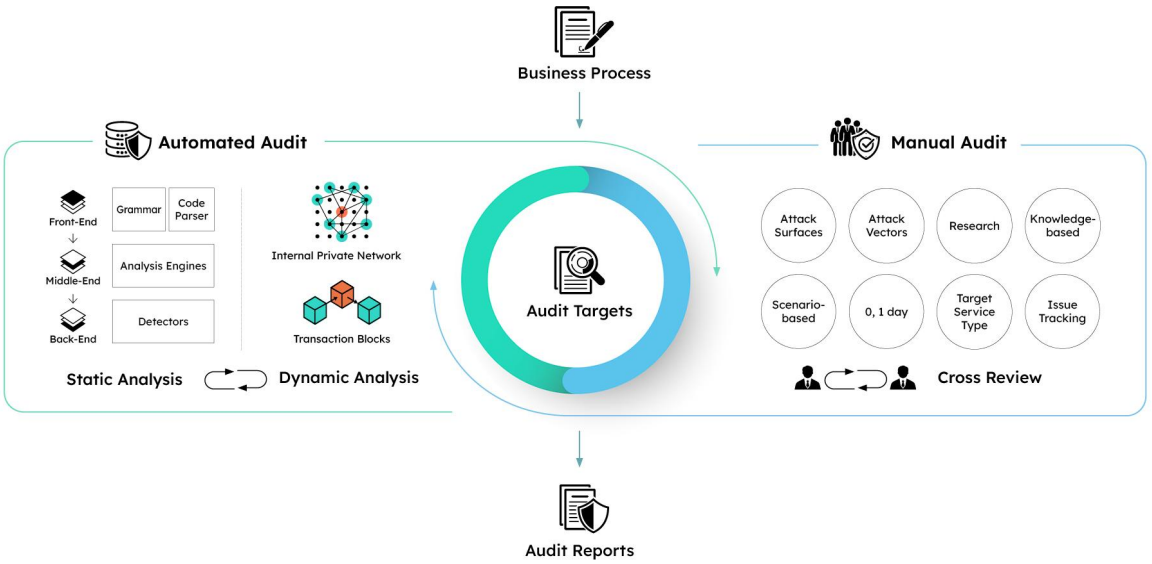
• SOOHO는 회사 정보가 대외비 이상의 성격을 가짐을 인지하고 사전 승인 없이 이를 공개하지 않습니다.

• SOOHO는 업무 수행 과정에서 취득한 일체의 회사 정보를 누설하거나 별도의 매체를 통해 소장하지 않습니다.

• SOOHO는 스마트 컨트랙트 분석에 최선을 다하였음을 밝히는 바입니다.

1.2 SOOHO 보안 감사 프로세스

SOOHO는 자동 분석(Automated Audit)과 수동 분석(Manual Audit)의 두 가지 감사 방법론을 적용하여 더욱 완벽한 블록체인 보안 감사를 진행합니다.



자동 분석은 정적 분석(Static analysis)과 동적 분석(Dynamic analysis) 사이 상호 협력적 분석을 통해 다양한 공격을 정확하고 빠르게 찾아내며 높은 감사 퀄리티를 보장합니다. SOOHO의 자체 분석기는 정적 분석을 통해 고객사 컨트랙트 코드의 문법을 분석(parsing)하여 의미 추론, 변수 추적, 경로 탐색을 진행함으로써 조건을 검증합니다. 정적 분석에서는 SOOHO 자체 테스트 네트워크에서 실제 동작을 통한 분석과 퍼징(Fuzzing), 콘콜릭 실행(Concolic Execution)을 통해 더욱 정교한 분석을 진행합니다.

수동 분석에서는 SOOHO의 보안 감사 전문가 그룹이 다양한 보안 및 도메인 지식을 활용하여 고객사의 프로젝트를 직접 검증합니다. 보다큰 리스크를 내포하는 코드를 중점적으로 분석하고, 파트너 사가 의도한 대로 코드가 작성되었는지 살피며 접근 권한의 관리가 올바르게 기능하고 있는지 검사합니다. 보안 감사 전문가들은 복잡한 공격 시나리오나 최근 보안 이슈를 처리하며 자동 분석을 상호 보완하여 감사의 완성도를 높입니다. 또한, 전문가 사이의 교차 검증을 통해 더욱 정교한 보안 감사 결과물을 제공합니다.

위와 같이 다양한 방법론을 이용하여 리스크 검증을 진행함으로써 파트너 사의 컨트랙트를 알려진 취약점 (1-day)과 0-day 취약점의 위협으로부터 안전하게 만들어줍니다.

발견된 취약점은 심각도 척도를 기준으로 하여 등급이 매겨집니다. 심각성 척도는 OWASP의 Impact & Likelihood 기반 리스크 평가 모델을 기반으로 정해졌습니다.

2. 분석 내용

‘분석 내용’ 파트에서는 NuriFlex Smart Contract 보안 감사 결과에 대한 전반적인 요약과 발견된 취약점의 구체적인 내용을 서술합니다. 발견된 모든 취약점에 대해 개선하는 것을 권장드리고 앞으로도 꾸준한 코드 감사를 통하여 서비스의 안정을 도모하시길 바랍니다.

2.1 분석 대상

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

2.2 분석 결과 요약

심각도 등급	취약점 수
Critical	
High	
Medium	
Low	
Note	

#	설명	심각도 등급	상태
SH-001	SafeMath 라이브러리를 제거하는 것을 통해 가스비를 아낄 수 있습니다.	Note	인지됨

주요 감사 포인트

NuriFlex는 NuriFlex World PTE., LTD.에서 개발한 BEP20 토큰입니다. 따라서 SOOHO Audit은 해당 컨트랙트 코드가 BEP20 표준에 잘 맞추어 작성되었는지, 통상적인 컨트랙트 보안 취약점은 존재하지 않는지, Gas의 낭비가 존재하지 않는지 등을 중점적으로 감사하였습니다.

단, 관리자의 내부 해킹을 비롯해 컨트랙트 외부 서버 환경의 안정성은 고려하지 않았습니다. 본 보고서에서는 언급하지 않았지만 노드 자체에 대한 보안 검증과 외부 연동되는 서비스에 대해서도 검토하기를 제안합니다. 분석은 대상 프로젝트에 포함된 컨트랙트의 기능 안정성에 관한 것입니다.

2.3 분석 결과

Note **SafeMath 라이브러리를 제거하는 것을 통해 가스비를 아낄 수 있습니다.**

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

Details

Solidity Version 0.8.0 이후 버전에서는 실행 환경에 의하여 더이상 Arithmetic Overflow/Underflow 취약점이 발생하지 않음이 보장됩니다. 따라서, Arithmetic Overflow/Underflow 취약점을 차단하는 SafeMath의 사용은 코드 용량을 증대시켜 컨트랙트 배치 시의 가스비와 매번 실행되는 코드의 양을 증가시켜 실행 가스비의 낭비를 초래합니다.

Mitigation

Solidity Version을 0.8.0 이상으로 조정하고 (현 최신 버전은 0.8.15) SafeMath 라이브러리와 그 적용 부분 코드를 수정하여 가스 낭비를 줄이시기를 권장합니다.

Update

NuriFlex 팀은 Solidity Version을 0.8.15로 조정하였습니다. 하지만, SafeMath 라이브러리를 제거하지는 않았으므로, 가스 최적화 이슈는 여전히 남습니다.

✔ (Verified) BEP20 Specification

Details

BEP20 표준을 따르는 것을 확인하였습니다. 특히, BEP20 표준 구현체를 적극 활용하여 업계의 권장 패턴을 적용하였음을 확인하였습 니다.

✔ (Verified) SWC-100

Details

스마트 컨트랙트에서 발생할 수 있는 함수 접근 범위에 대한 부분에 대한 검증을 완료하였습니다.

✔ (Verified) SWC-101

Details

정수형 데이터에 대한 오버플로우와 언더플로우 문제는 발생하지 않는 것을 확인하였습니다.

✔ (Verified) SWC-104

Details

호출 데이터에 대한 예외 처리가 포함되어 있습니다.

✔ (Verified) SWC-107

Details

Reentrancy 취약점이 발생하지 않음을 확인하였습니다.

✔ (Verified) SWC-108

Details

컨트랙트 클래스에 대한 설계가 잘 되어 있습니다.

✔ (Verified) SWC-113

Details

DoS는 발생하지 않습니다.

✔ (Verified) SWC-118

Details

생성자 이름은 모두 온전하게 작성되어 있습니다.

2.4 결론

NuriFlex World PTE., LTD.에서 개발한 NuriFlex 컨트랙트는 이해하기 쉽게 명명되고 용도와 쓰임에 따라 잘 설계되어 있습니다. 대부분 모범 사례를 따르고 있습니다. 컨트랙트들은 매우 잘 설계되었고 그 구현 또한 훌륭하였음을 강조하고 싶습니다.

코드 검사 결과 발견된 이슈는 **Note 1개** 입니다. 꾸준한 코드 감사를 통해 컨트랙트의 안정을 도모하고 잠재적인 취약점에 대한 분석을 하는 것을 추천드립니다.

About SOOHO

SOOHO는 블록체인 생태계의 안전성과 신뢰도를 높이기 위한 기술을 연구하고 제공하고자 시작하였습니다. SOOHO는 자체적으로 개발한 취약점 분석기와 오픈 소스 분석기로 스마트 컨트랙트 취약점을 검증합니다. 더하여, SOOHO의 보안팀은 Defcon, Nuit du Hack, 화이트햇, SamsungCTF 등 국내외의 해킹 대회에서 수상하고, 보안분야 박사 학위와 같은 학문적 배경을 가지는 등 우수한 해킹 실력과 경험을 가진 보안 전문 인력들로 구성되어 있습니다. SOOHO의 전문 전문가들은 알려진 1-DAY 취약점부터 0-DAY 취약점으로부터 고객사의 스마트 컨트랙트를 보호하고자 합니다.

Contact us :)

Twitter: SOOHO_AUDIT

E-mail: audit@sooho.io

Website: https://audit.sooho.io/