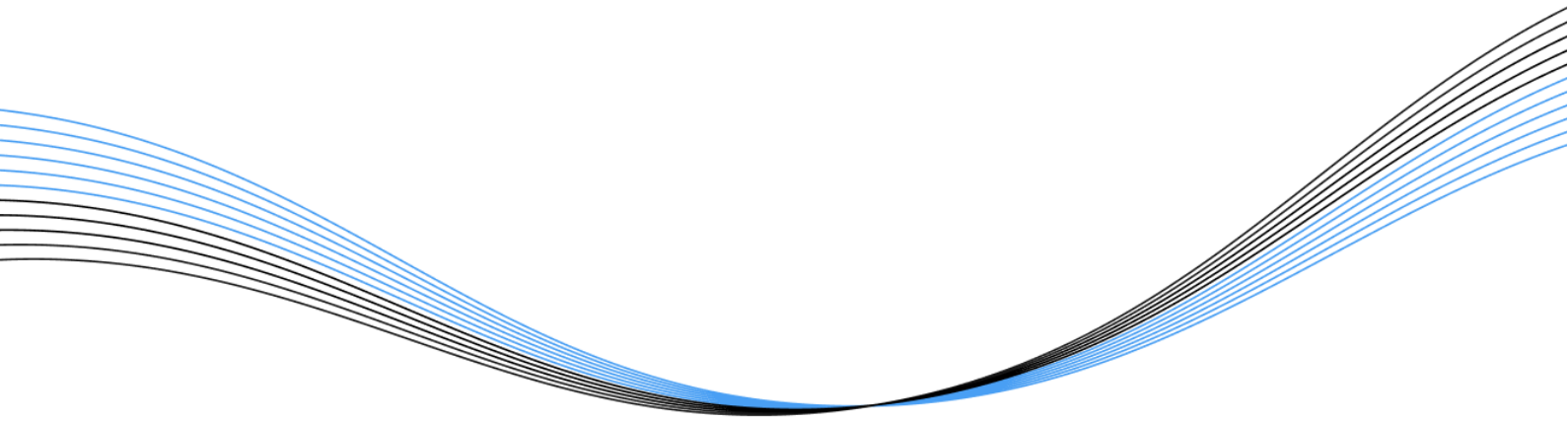
© Hexlant Inc.
Gangnam-daero 340
Seoul,
Republic of Korea 06242
Hexlant.com

INC SMART CONTRACT AUDIT REPORT



Audit Date
8 JUN 2021

Category
Token Contract

Auditor
Hexlant Audit Team

This contract specifies that it has been validated by the Hexlant Technical Team and notifies that it has not any technical defects.

AUDIT OVERVIEW

PUBLISHED INFORMATION	
REPORT NUMBER	ERC20210608
DATE	2021/06/08
PUBLISHER	Henry / henry@hexlant.com

PROJECT INFORMATION			
TITLE	InstaCoin		
SYMBOL	INC		
PLATFORM	ETHEREUM	**TOKEN TYPE**	ERC-20
TOTAL SUPPLY	2,000,000,000 INC ⋆'100억 INC 발행, 80억 INC burn address로 전송하여 소각'		
CONTRACT ADDRESS	0xa21e70bc68234acf336f3bf2be3c5a039a3476e2		

VULNERABILITY ANALYSIS		
CRITICAL	0	-
HIGH	0	-
MEDIUM	3	Pause, Freeze, Lockup
LOW	1	SafeMath

CENTRALIZED FUNCTION		
FREEZE	NO	Ability to freeze tokens in accounts. (The administrator can freeze the hacker's account in case of hacking.)
PAUSE	NO	Ability to pause functions related to token transmission in a contract. (This is used when the administrator needs to prevent the movement of assets due to token swaps or hacking.)
LOCKUP	NO	Ability to block token transfers for a period of time (Administrators can use to set lockout periods for investors, team members, advisors, etc.)
BURN	NO	Ability to reduce total supply by burning tokens
MINT	NO	Ability to increase total supply by minting tokens

COMPANY PROPOSAL

Hexlant는 2018년에 설립한 블록체인 기술 기업입니다. 삼성전자 출신의 보안·네트워크·소프트웨어 전문가가 스마트 컨트랙트와 블록체인 프로토콜의 보안 결함을 발견하고 블록체인 생태계의 기술 안정성을 입증하기 위해 설립하였습니다.

Hexlant는 블록체인 동작 환경을 파악하기 위해 20개 이상의 블록체인 메인넷을 직접 구축하고 있습니다. 나아가 키 보안 알고리즘 및 메인넷 모니터링 기술을 개발했습니다. 이 방식은 비트코인, 이더리움, 폴카닷, 에이다 등 헥슬란트가 보유한 모든 메인넷 플랫폼에서 적용되고 운영됩니다.

Hexlant는 위와 같은 기술 운영 경험을 바탕으로 스마트 컨트랙트 기술을 검증합니다. 스마트 컨트랙트 내 버그를 발견하는 오류 테스트 뿐만 아니라 메인넷 상황에서의 문제점을 탐지하며 서비스 관점에서 지속적으로 운영할 수 있는 블록체인 기술 가이드를 제공합니다.

Hexlant의 고객사는 컨트랙트에 대한 취약성 감사부터 오너 키 관리, 블록체인 지갑 시스템 구축 등 블록체인 기술 전반의 서비스를 제공받을 수 있습니다. 현재 200여개의 고객사가 Hexlant의 서비스를 바탕으로 블록체인 사업을 시작, 운영했으며 누적으로 관리하는 자산은 12조를 달성했습니다.

Initials for identification purposes:

CONTENTS

ANALYSIS PURPOSE

본 리포트는 발행된 컨트랙트 코드가 요구사항을 충분히 만족하는지, 그리고 보안의 취약점과 실제 운영 하면서 발생 할 수 있는 문제들을 파악하고 해결방안을 찾기위해 분석을 수행하고 그 결과를 정리하였습니다. 이번 코드 분석은 다음과 같은 요소들을 검증하기위해 진행하였습니다.

- 구현된 기능의 정상 작동 여부
- 기능 수행 중 보안 위험성
- Off Chain에서 발생하는 문제에 대한 대비
- 컨트랙트 코드의 가독성 및 코드 완성도

VULNERABILITY CLASSIFICATION

본 취약성 검증은 오류 위험도를 아래와 같이 분류, 평가합니다.

● Critical Severity

심각성 치명적 단계는 큰 보안 결함을 뜻하며 자산 탈취 및 동결, 추가 발행 등 치명적인 문제를 야기합니다. 본 결함은 반드시 수정되야 합니다.

● High Severity

심각성 높은 단계는 특수 조건에 의해 보안 결함이 발생할 수 있는 항목이며 수정을 강력하게 권고합니다.

● Medium Severity

심각성 중간 단계는 보안 결함은 아니나 비효율적인 컨트랙트 동작을 야기합니다. 컨트랙트를 효율적으로 동작하도록 수정을 권유하는 항목입니다.

● Low Severity

심각성 낮음 단계는 보안에는 문제가 없으나 컨트랙트 구조 개선을 위해 수정을 권유하는 항목입니다.

INC CONTRACT VULNERABILITY ANALYSIS		
● **CRITICAL**	0	-
● **HIGH**	0	-
● **MEDIUM**	3	Pause, Freeze, Lockup
● **LOW**	1	SafeMath

FUNCTION SUMMARY

Function 1. Contract

상태 변수와 함수를 포함하여 컨테이너 형태의 계약을 표현하기 위해 사용

Contract	Description
InstaCash	INC 토큰 컨트랙트

Function 2. Interface

컨트랙트 내 구현하고자 하는 표준함수를 정의하기 위해 사용

Interface	Description

Function 3. Library

상태 변수를 가질 수 없고 상속을 지원하지 않는 컨트랙트 라이브러리. 라이브러리 함수가 호출되며 호출한 컨트랙트의 컨택스트에서 실행

Library	Description
SafeMath	산술 연산 제어

Function 4. Variable

컨트랙트의 상태를 표현하는 변수들로 컨트랙트에 필요한 정보들을 저장하기 위해 사용

Variable	Description
balanceOf	특정 주소의 토큰 잔액 테이블
totalSupply	토큰 총 발행량
name	토큰 이름
symbol	토큰 심볼
decimals	토큰 데시멀
allowance	특정 주소의 토큰 출금 허용 잔액

Function 5. Modifier

함수의 한정요소로 특정 기능을 수행할 때 한정된 조건에서만 실행될 수 있도록 하기 위해 사용

Modifier	Description

Function 6. Event

컨트랙트 함수 실행에 따른 로그 이벤트로 추후 애플리케이션 적용에 있어 컨트랙트 상황을 보다 쉽게 대응하기 위해 사용

Event	Description
Transfer	토큰 전송 시 이벤트 발생
Approval	출금 위임 시 이벤트 발생

Function 7. Function

컨트랙트의 함수들로써 컨트랙트에 필요한 특정 로직을 담아 기능 실행을 하기 위해 사용

Function	Description
approve	특정 주소에게 출금 위임
transfer	토큰 전송
transferFrom	출금 위임된 토큰 전송

TEST RESULT

Code Coverage

코드 커버리지는 작성한 테스트가 얼마만큼 컨트랙트 코드의 기능을 테스트 했는지 알 수 있는 정량적인 지표입니다.

INC 컨트랙트는 라이브러리와 일부 컨트랙트에 구현된 기능에 대해 추가적인 호출이 진행되지 않은 경우가 존재합니다.

아래의 Coverage 지표는 위 사항을 반영한 결과입니다.

File Name	Statements	Functions	Lines
CTPL.sol	100% (22/22)	100% (6/6)	100% (17/17)

TEST CASE

실제 적용한 테스트케이스 목록입니다.

Test Case	Result	
배포 시 지정한 토큰의 이름과 일치하는가?	PASS	FAIL
배포 시 지정한 토큰의 심볼과 일치하는가?	PASS	FAIL
배포 시 지정한 토큰의 데시멀과 일치하는가?	PASS	FAIL
배포 시 지정한 토큰의 초기 발행량과 일치하는가?	PASS	FAIL
배포 시 지정한 초기 발행량이 컨트랙트 배포자에게 할당되는가?	PASS	FAIL
배포 후 오너 외의 주소에 토큰잔액은 0인가?	PASS	FAIL
기본적인 토큰 전송은 잘 동작하는가?	PASS	FAIL
특정 주소들의 올바른 토큰 잔액을 반환한다.	PASS	FAIL
보유 토큰 잔액을 초과하여 토큰 전송 시 예외처리가 되는가?	PASS	FAIL
받는 주소가 0x0의 주소일 경우, 예외처리가 되는가?	PASS	FAIL
토큰에 대한 출금을 위임할 수 있는가?	PASS	FAIL
출금 위임된 토큰의 잔액을 확인 가능한가?	PASS	FAIL
출금 위임된 토큰을 전송 가능한가?	PASS	FAIL
출금 위임된 토큰을 전송 시 받는 주소가 0x0일 경우 예외처리가 되는가?	PASS	FAIL
출금 위임된 토큰을 전송 시 위임자의 잔액이 부족할 경우 예외처리가 되는가?	PASS	FAIL
출금 위임된 토큰을 전송 시 위임된 잔액을 초과하여 전송 시 예외처리가 되는가?	PASS	FAIL

VULNERABILITY ANALYSIS

INC CONTRACT VULNERABILITY ANALYSIS		
● **CRITICAL**	0	-
● **HIGH**	0	-
● **MEDIUM**	3	Pause, Freeze, Lockup
● **LOW**	1	SafeMath

➢ **MEDIUM- 01 :** 전체토큰에 대한 거래 정지 기능

Type	Severity	Location
Recommend	● **MEDIUM**	-
· Description :	메인넷 스왑이나 탈 중앙화 거래소를 통한 상장 이슈 등과 관련하여 Pausable 토큰으로 발행하는 것을 고려할 수 있습니다. Pauseble 토큰의 경우 Pause 시킬경우, 토큰의 전송이 모두 막히게 됩니다. 이를 통해 메인넷 스왑 기간동안, 토큰의 이동을 막은 상황에서 스냅샷 생성이 용이해 집 니다. 또한 이 기능을 활용하여, 원치않는 시기에 탈 중앙화 거래소에서 거래가 불가능 하도록 만들 수도 있습니다. 다만 오너의 권한으로 토큰을 통제한다는 것이 탈 중앙화에 위배된다는 이슈도 있습니다. 이 부분은 INC Token의 정책에 따라 결정하시길 권유드립니다.	

➢ **MEDIUM 02 :** 개별 주소에 대한 **Freeze**

Type	Severity	Location

Unnecessary Operation	● MEDIUM	-
· Description :	최근 거래소 해킹사태가 종종발생하고 있으며, 피싱사이트 등을 통해 토큰 홀더들의 토큰들이 탈취되는 일들이 발생 하고 있습니다. 거래소의 해킹등으로 대량의 토큰이 탈취당할 경우, 탈취물량의 매도로 인해 토큰 가격이 폭락 할 수 있습니다. 만일의 사태에 대비하여 탈취된 물량을 동결 시킬수 있도록, 개별주소에 Freeze를 걸 수 있는 기능을 고려할 수 있습니다. 다만 오너의 권한으로 개별 락업 거는 것이 탈중앙화에 위배된다는 이슈도 있습니다. 이 부분은 INC Token의 정책에 따라 결정하시길 권유드립니다.	

➢ **MEDIUM- 03 :** 개별 주소에 대한 **Lockup**

Type	Severity	Location
Unnecessary Operation	● MEDIUM	-
· Description :	투자자, 팀원 및 어드바이저 등 토큰을 분배하는 경우, 전송 시점 부터 언제든 해당물량이 시장에 한번에 나와 가격이 폭락 할 수 있습니다. 이런 경우 Lockup 을 활용하여 시간에 따라 시장에 분배되는 토큰의 양을 조절할 수 있습니다. 다만 오너의 권한으로 개별 락업 거는 것이 탈중앙화에 위배된다는 이슈도 있습니다. 이 부분은 INC Token의 정책에 따라 결정하시길 권유드립니다.	

➢ **LOW- 01 : SafeMath**

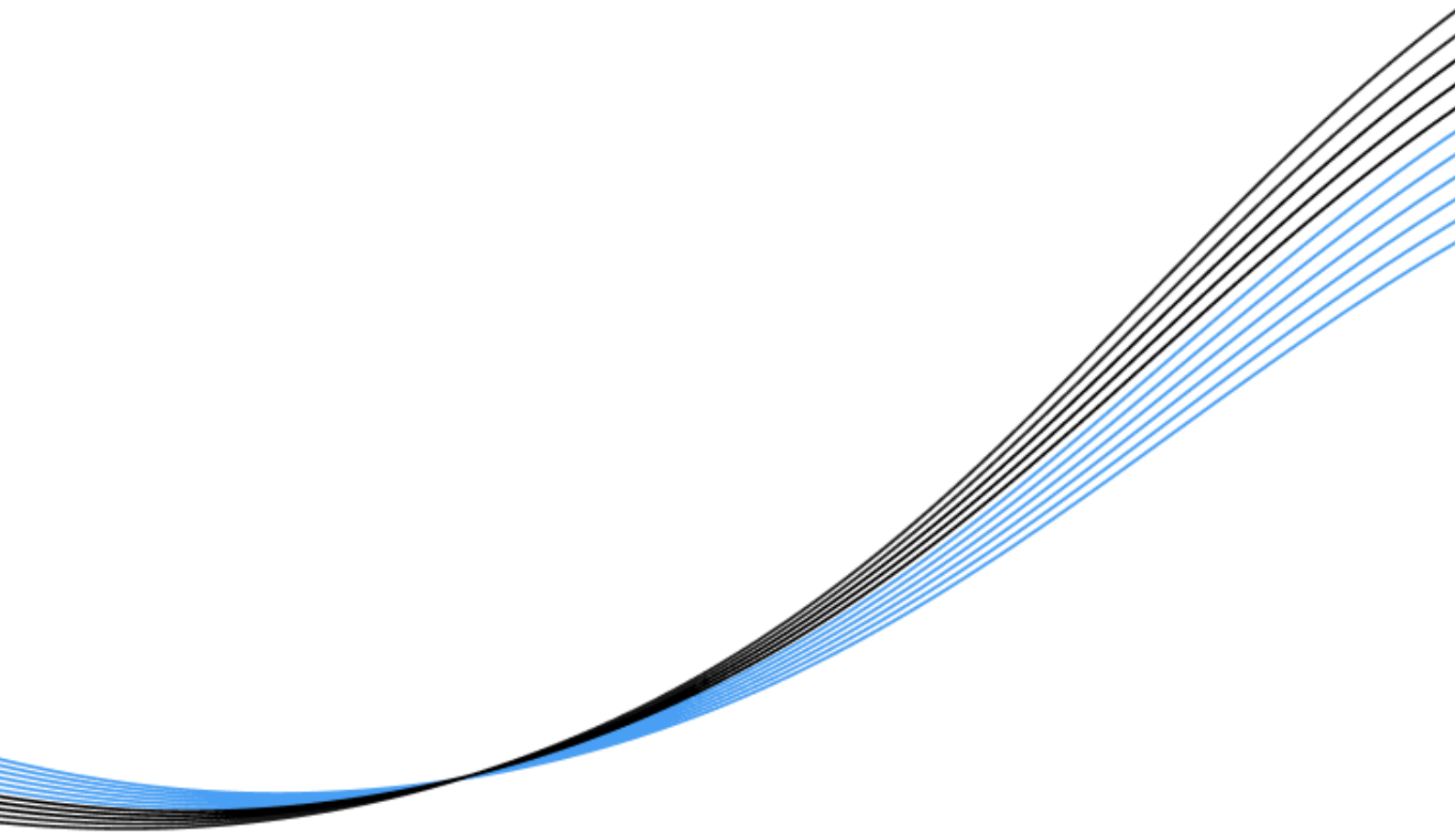
Type	Severity	Location
typo	● LOW	-
· Description :	Solidity 0.8 버젼 이상부터는 연산자 (+, -, /, %등) 계산에 의한 언더플로와 오버플로에 대해 Revert 하는 기능이 추가 되었습니다. SafeMath 를 사용한다고 해서 큰 문제가 있는 것은 아닙니다.	
· Recommendation :	add, sub 는 +, - 로 대체 하는것을 추천드립니다.	

CONCLUSION

INC 컨트랙트는 최신 솔리디티 버젼을 사용하여 만들어진 컨트랙트 입니다. 헥슬란트가 진행한 모든 TEST CASE를 통과 하였습니다. 다만 Pause나 Freeze 등의 기능 부재로 토큰 해킹 이나 오입금 시 피해를 입을 수 있습니다.

Declare

해당 리포트는 Hexlant의 스마트 컨트랙트 보안 감사 결과를 바탕으로 작성되었습니다. 해당 리포트는 비즈니스 모델의 적합성과 법적 규제, 투자에 대한 의견을 보증하지 않습니다. 리포트에 기술한 문제점 이외에 메인넷 기술 또는 가상머신을 비롯하여 발견되지 않은 문제점이 있을 수 있습니다. 해당 리포트는 논의 목적으로만 사용됩니다.



Hexlant.

-

contact@hexlant.com
www.hexlant.com