3rd MARCH 2021

SMART CONTRACT AUDIT REPORT

-

version v2.0

Smart Contract Security Audit and General Analysis

HAECHI AUDIT

Table of Contents

1 Issues (1 Critical, 0 Major, 0 Minor) Found

About HAECHI AUDIT

HAECHI AUDIT은 글로벌 블록체인 업계를 선도하는 HAECHI LABS의 대표 서비스 중 하나로, 스마트 컨트랙트 보안 감사 및 개발을 전문적으로 제공합니다.

다년간 블록체인 기술 연구 개발 경험을 보유하고 있는 전문가들로 구성되어 있으며, 그 전문성을 인정받아 블록체인 기술 기업으로는 유일하게 삼성전자 스타트업 육성 프로그램에 선정된 바 있습니다. 또한, 이더리움 재단과 이더리움 커뮤니티 펀드로부터 기술 장려금을 수여받기도 하였습니다.

HAECHI AUDIT의 보안감사 보고서는 전세계 암호화폐 거래소들의 신뢰를 받고 있습니다. 실제로 많은 클라이언트들이 HAECHI AUDIT 스마트 컨트랙트 보안감사를 거친 후에, Huobi, OKEX, Upbit, Bithumb 등에 성공적으로 상장하였습니다.

대표적인 클라이언트 및 파트너사로는 글로벌 블록체인 프로젝트와 포춘 글로벌 500대 기업들이 있으며, 카카오의 자회사인 Ground X, Carry 프로토콜, Metadium, LG, 한화, 신한은행 등이 있습니다. 지금까지 약 60여곳 이상의 클라이언트를 대상으로 가장 신뢰할 수 있는 스마트 컨트랙트 보안감사 및 개발 서비스를 제공하였습니다.

문의 : audit@haechi.io
웹사이트 : audit.haechi.io

01. Introduction

본 보고서는 아이템게임즈 팀이 제작한 BSCBridge 스마트 컨트랙트의 보안을 감사하기 위해 작성되었습니다. HAECHI AUDIT 는 아이템게임즈 팀이 제작한 스마트 컨트랙트의 구현 및 설계가 공개된 자료에 명시한 것처럼 잘 구현이 되어있고, 보안상 안전한지에 중점을 맞춰 감사를 진행했습니다.

발견된 이슈는 중요도 차이에 따라 CRITICAL, MAJOR, MINOR, TIPS 로 나누어집니다.

CRITICAL	Critical 이슈는 광범위한 사용자가 피해를 볼 수 있는 치명적인 보안 결점으로 반드시 해결해야 하는 사항입니다.
MAJOR	Major 이슈는 보안상에 문제가 있거나 의도와 다른 구현으로 수정이 필요한 사항입니다.
MINOR	Minor 이슈는 잠재적으로 문제를 발생시킬 수 있으므로 수정이 요구되는 사항입니다.
TIPS	Tips 이슈는 수정했을 때 코드의 사용성이나 효율성이 더 좋아질 수 있는 사항입니다.

HAECHI AUDIT는 아이템게임즈 팀이 발견된 모든 이슈에 대하여 개선하는 것을 권장합니다.

이어지는 이슈 설명에서는 코드를 세부적으로 지칭하기 위해서 {파일 이름}#{줄 번호}, {컨트랙트 이름}#{함수/변수 이름} 포맷을 사용합니다. 예를 들면, *Sample.sol:20*은 Sample.sol 파일의 20번째 줄을 지칭하며, *Sample#fallback()* 는 Sample 컨트랙트의 fallback() 함수를 가리킵니다

보고서 작성을 위해 진행된 모든 테스트 결과는 Appendix에서 확인 하실 수 있습니다.

02. Summary

Audit에 사용된 코드는 Github (https://github.com/itamgames/bsc-bridge-core)에서 찾아볼 수 있습니다. Audit에 사용된 코드의 마지막 커밋은 "d7c58b8530fd7acbe74bd13a9c04bff4de97fa6a" 입니다.

Issues

HAECHI AUDIT에서는 Critical 이슈 1개, Major 이슈 0개, Minor 이슈 0개를 발견하였으며 수정했을 때 코드의 사용성이나 효율성이 더 좋아질 수 있는 사항들을 1개의 Tips 카테고리로 나누어 서술하였습니다.

Severity	Issue	Status
CRITICAL	**BSCBridge#transit(), ETHBridge#withdraw() 함수가 replay 공격에 취약합니다**	(Found v1.0) (Fixed v2.0)
TIPS	**널리 사용되는 ECDSA 라이브러리를 사용하십시오**	(Found v1.0) (Fixed v2.0)
Notice	**Signer 가 ETHBridge에서 마음대로 토큰을 인출 할 수 있습니다**	(Acknowledged)
Notice	**Owner 나 Signer 출금 요청을 무효화 할 수 있습니다**	(Acknowledged)
Notice	**Owner 가 ItamERC20 토큰을 무한히 발행할 수 있으며 사용자의 자산을 마음대로 소각 할 수 있습니다**	(Acknowledged)

Update

[v2.0] - 1 개의 critical, 개의 1 tips 가 새로운 커밋 해시
f7e951b35501ad8e7974795a55b80de454a35053 에서 해결 되었습니다

03. Overview

Contracts Subject to Audit

- BEP20.sol
- BSCBridge.sol
- ETHBridge.sol
- TransferHelper.sol

Roles

BSCBridge 스마트 컨트랙트에는 다음과 같은 권한이 있습니다

- **Owner**
- **Signer**

각 권한으로 접근 할 수 있는 기능은 다음과 같습니다.

Role	Functions
Owner	● BSCBridge ○ changeTransitFee ○ changeSigner ○ withdrawFee ○ transferTokenOwnership ● ETHBridge ○ changeSigner ● ItamERC20 ○ mint ○ burn
Signer	-

Notice

- **Signer 가 ETHBridge에서 마음대로 토큰을 인출 할 수 있습니다**

  ETHBridge스마트 컨트랙트는 ERC20 자산들을 lock up 하는 용도로 이용됩니다. 이 자산들은 withdraw() 함수로만 인출 할 수 있습니다. 이 때 이 함수를 호출하는 조건은 Signer의 privateKey로 signing 하는지 여부만 확인합니다. 따라서 Signer는 다른 조건 없이 ERC20 자산을 마음대로 인출 할 수 있습니다

  해당 이슈는 중앙화 이슈이며 아이템게임즈 측에서 이 이슈에 대해 인지하고 있다고 답변을 받았습니다.

- **Owner 나 Signer 출금 요청을 무효화 할 수 있습니다**

  아무리 사용자가 유효한 서명값을 발급 받더라도, Owner가 Signer 주소를 변경하거나, Signer가 중복된 withdrawId로 다른 출금 서명을 만들게 된다면 발급받은 서명값이 무효화 됩니다,

  해당 이슈는 중앙화 이슈이며 아이템게임즈 측에서 이 이슈에 대해 인지하고 있다고 답변을 받았습니다.

- **Owner 가 ItamERC20 토큰을 무한히 발행할 수 있으며 사용자의 자산을 마음대로 소각 할 수 있습니다**

  ItamERC20 컨트랙트에는 Owner만 호출 할 수 있는 mint(), burn() 함수가 존재합니다. mint() 함수를 이용하여 무한히 토큰을 발행할 수 있으며 사용자의 자산을 마음대로 소각 할 수도 있습니다. BSCBridge가 Owner로 지정되어있는경우 문제가 없으나 Owner가 변경되는경우 문제가 생길 수 있습니다.

  해당 이슈는 중앙화 이슈이며 아이템게임즈 측에서 이 이슈에 대해 인지하고 있다고 답변을 받았습니다.

04. Issues Found

CRITICAL : BSCBridge#transit(), ETHBridge#withdraw() 함수가 replay 공격에 취약합니다(Found - v1.0) (Resolved - v2.0)

CRITICAL

Problem Statement

BSCBridge#transit(), ETHBridge#withdraw() 함수들은 ecrecover 라는 방법을 통해 서명값과 메세지가 Signer에 의해 서명되었다는 것을 검증합니다. 하지만 이 때 사용하는 메세지의 형태가 두 함수에서 동일하여 같은 메세지/서명값을 이용하여 두 함수를 호출 할 수 있습니다.

Recommendation

서명 메시지 값에 블록체인을 구분짓는 chainId 값과, 사용되는 스마트 컨트랙트 주소를 추가 하십시오.

Update

[v2.0] - 아이템게임즈 팀에서 Recommendation 사항을 적용하여 문제가 해결되었습니다.

TIPS : 널리 사용되는 ECDSA 라이브러리를 사용하십시오 (Found - v1.0) (Resolved - v2.0)

TIPS

Problem Statement

BSCBridge#_recoverAddress(), ETHBridge#_recoverAddress() 함수에 ecrecover 함수를 이용해 서명값에서 서명한 주소를 추출하는 로직이 구현되어있습니다. 널리 사용되는 ECDSA 라이브러리를 사용하여 코드의 안전성을 높이는 것을 추천드립니다.

Update

[v2.0] - 아이템게임즈 팀에서 openzeppelin에서 사용되는 ecdsa 라이브러리로 변경하여 이슈가 해결되었습니다.

05. Disclaimer

해당 리포트는 투자에 대한 조언, 비즈니스 모델의 적합성, 버그 없이 안전한 코드를 보증하지 않습니다. 해당 리포트는 알려진 기술 문제들에 대한 논의의 목적으로만 사용됩니다. 리포트에 기술된 문제 외에도 이더리움, 솔리디티 상의 결함 등 발견되지 않은 문제들이 있을 수 있습니다. 안전한 스마트 컨트랙트를 작성하기 위해서는 발견된 문제들에 대한 수정과 충분한 테스트가 필요합니다.