July25(th)y2021

FUTURE GLOBAL VILLAGE

SMART CONTRACT

AUDIT REPORT

versionv.O

SmartContractSecurityAuditand General Analysis

HAECHI AUDIT

Table ofContents

About FGVAUDIT

FGV AUDITisaglobal leading smart contract security audit and development firm operated by FGV LABS. FGV AUDIT consists of professionals with years of experience in blockchain R&Dand providesthemostreliablesmartcontractsecurityaudit and developmentservices.

Sofar, based on the FGVAUDIT's securityaudit report, ourclients have been successfullylistedontheglobalcryptocurrencyexchangessuchasHuobi, Upbit,OKEX, and others.
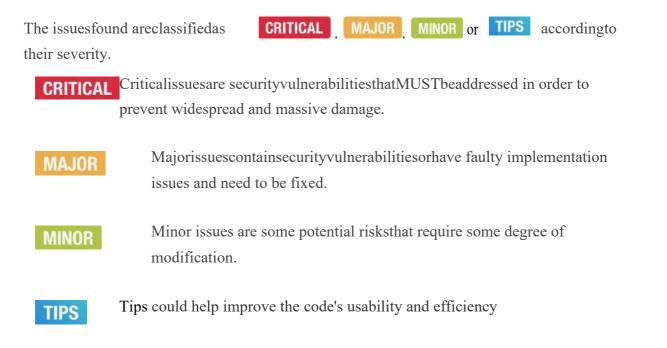
Ournotable portfolios includeSKTelecom, GroundXby Kakao, andCarry Protocolwhile FGVAUDIThasconducted securityauditsfortheworld'stopprojectsandenterprises.

Trusted bythe industry leaders, we have been incubated bySamsung Electronics and awarded the Ethereum Foundation Grants and Ethereum CommunityFund.

Contact: audit@FGV.io
Website : audit.FGV.io

01. Introduction

This report was written to provide a security audit for the Future Global Villag smart contract. FGV conducted the audit focusing on whether Future Global Villag smart contract is designedand implemented inaccordancewith publiclyreleased informationandwhether it has any security vulnerabilities.

The issuesfound areclassifiedas **CRITICAL** , **MAJOR** , **MINOR** or **TIPS** accordingto their severity.

CRITICAL Criticalissuesare securityvulnerabilitiesthatMUSTbeaddressed in order to prevent widespread and massive damage.

MAJOR Majorissuescontainsecurityvulnerabilitiesorhave faulty implementation issues and need to be fixed.

MINOR Minor issues are some potential risksthat require some degree of modification.

TIPS Tips could help improve the code's usability and efficiency

FGV AUDIT advises addressing all the issues found in this report.

02. Summary

Issues

FGV AUDIT has 0 Critical Issues, 0 Major Issues, and 2 Minor Issue.

Severity	Issue	Status
	Future Global Villag#delegateBySig() can be called with (nonce, expiry) which was not used to generate the (v, r, s).	(Found v1.0)
MINOR ■	**Space Station,VaultFlipToCake#notifyRewardAmount() can decrease rewardRate**	(Found v1.0) (Intended Behavior- v2.0)
NOTICE	**Non-audited, changeable external contract**	(Found v1.0)

03. Overview

Contracts Subject to Audit

- Future Global Villag.sol
- Future Global VillagToken.sol
- Space Station.sol
- Future Global VillagTRXPool.sol
- VaultCakeToCake.sol
- VaultFlipToFlip.sol
- VaultFlipToCake.sol

Roles

The Future Global Village Smart contract has the following authorizations:

- **Owner**
- **Minter**
- **Keeper**
- **RewardDistribution**

The features accessible by each level of authorization is as follows:

Role	Functions

Owner	• Future Global VillagToken
	   o mint
	• VaultFlipToCake
	   o setMinter
	   o setRewardsToken
	   o setRewardsDuration
	   o recoverToken
	• Future Global VillagMinter
	   o transferFuture Global Villag o setWithdrawalFee
	   o setPerformanceFee
	   o setWithdrawalFeeFreePeriod
	   o setMinter
	   o setFuture Global VillagTRX
	   o setFuture Global VillagPerFuture Global VillagTRXFIip

	o setHelper
	  • VaultController
	   o setMinter
	   o recoverToken
	  • VaultFlipToFlip
	   o recoverToken
	  • Space Station
	   o setRewardsToken
	   o setHelper
	   o recoverBEP20
	   o setRewardsDuration
	  • Future Global VillagTRXPool
	   o setFlipToken
	   o setMinter
	   o setHelper

Minter	• Future Global VillagMinter
	   o mintFor
	   o mintForFuture Global VillagTRX

Keeper	• VaultController
	   o setKeeper
	  • VaultFlipToFlip
	   o harvest

RewardDistributio n	• VaultFlipToCake
	   o notifyRewardAmont
	  • Space Station
	   o notifyRewardAmount

Notice

- Non-audited, changeable external contract

FGV has found that Future Global Villag protocol used "StrategyHelper" contract in several partsforgettingtvl,apy.Althoughthis helperisusedtogetdata, not writingdatawhich is much safer. Butthis"helper"can bechanged bytheowner andthiscan leadtoprice manipulation.Also,theseviewfunctionswhichdependon helper contracts, are weak to flash loan attacks. Do nottrustthese functions as a price tablewhen building on top of this protocol.

Ifyouareanend-user,this issuewill notexpose much issue/securityrisktoyou. Butifyou build somethingon topofthiscode, be aware oftheabove issue.

04. Issues Found

MMINOR: Future Global Villag#delegateBySig() can be called with (nonce, expiry) which was not used to generate the (v, r, s). (Found - v1.0)

MINOR

Problem Statement

Future Global Villag#delegateBySIg() is designed to delegate the voting right with meta-transaction. Inthiscase,thedelegatorgenerates(v, r,s)bysigning(nonce,expiry) with its privateKey. Delegatee(oranyotheronewhocan callthisfunction)willcall delegateBySig()withtheseparameter.Thenthefunctionshouldverifyifthe(v,r,s)is signed bydelegator, butinFuture Global Villag, itdoes notcheckifthesigneristhedelegator. Whichwill resultindelegating anotheraddress's voting power instead ofthedelegator if (nonce, expiry) is not the one that was signed.

Recommendation

Add one more parameterindelegateBySig()functionthatgetsdelegator'saddressand verify if ecrecovered address is delegator.

Disclaimer

- **This issue has been found on most well-known governance tokens, since these "delegate" parts are copyand pasted which resu ltsinalmostthe same codes being used over and over again.**
- **Although this looks very malicious, it is nearly impossible to find (nonce,expiry) that will result in making another user with voting power to delegate instead of the actualsigner.**
- **If you are an end-user, thisissuewillnotexposemuchissue/securityriskto you. But ifyou aregoingto build on top ofthiscode, such as openingawebsite to receive voting powerusing delegateBySig, orsomekindof reward system contract that rewards users when delegate, be aware that this "delegateBySig" won't guarantee the signature is valid.**

MINOR:Space Station,VaultFlipToCake#notifyRewardAmount()candecrease

rewardRate (Found - v1.0) (Intended Behavior - v2.0)

MINOR

Problem Statement

notifyRewardAmount() does not check if the rewardRate decreases after notification.
Since it updates rate to be *(leftoverRate + notifiedreward)/duration* when previous reward is notfinished, ifadmin keeps notifying withzero reward, itcan leadtocontinuousdecrease on reward rate,

Sincethisfunction is designed tobe only called byadmin, this error canonlybedone by admin.

ReFuture Global Villag commendation

Check if rewardRate increases after notifying reward.

Update

 team has confirmed that this is a intended behavior

05. Disclaimer

This report is notan advice on investment, nordoes it guarantee adequacy of a business modeland/orabug-freecode.Thisreportshould beusedonlytodiscussknowntechnical problems.ThecodemayincludeproblemsonEthereumthatarenotincluded inthis report.ltwillbenecessarytoresolveaddressedissuesandconductthoroughteststo ensure the safety of the smart contract.