incrypto

Smart-contract audit & code review

Project: GETETH
Date: March, 5 , 2019

Table of contents

Abstract

In this report, we consider the security of the InvestToken, GameWithToken contracts. Our task is to find and describe security issues in the smart contracts of the platform. This report presents the findings of the security assessment of Customer`s smart contract and its code review conducted between February 28th, 2019 - March 05th, 2019

Disclaimer

The audit does not give any warranties on the security of the code. One audit can not be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, security audit is not an investment advice.

Scope

The scope of the project is GetToken and Game smart contracts:

1. InvestToken

2. GameWithToken

We have scanned this smart contracts for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered (the full list includes them but is not limited to them):

- Unsafe type inference

- Timestamp Dependence
- Reentrancy
- Implicit visibility level
- Gas Limit and Loops
- Transaction-Ordering Dependence
- Unchecked external call – Unchecked math
- DoS with Block Gas Limit
- DoS with(Unexpected) Throw
- Byte array vulnerabilities
- Malicious libraries
- Style guide violation
- ERC20 API violation
- Uninitialized state/storage/local variables
- Compile version not fixed

Procedure

In our report we checked the contracts with the following parameters:

- Whether the contracts is secure.
- Whether the contracts corresponds to the documentation.
- Whether the contracts meets best practices in efficient use of gas, code readability.

We perform our audit according to the following procedure:

Automated analysis:

- Scanning contracts by several public available automated analysis tools such as Mythril, Slither.
- Manual verification all the issues found by tools

Manual audit:

- Manual analysis smart contracts for security vulnerabilities
- Checking smart contracts logic and comparing it with one described in the documentation

AS-IS overview

InvestToken contract overview

InvestToken contract constructor sets:

bonusToken to instance of BonusToken().

gameAddress to _gameAddress.

swapTokensLimit to 10000.

divider to _divider.

InvestToken has 1 modifier:

onlyGame - check that msg.sender is gameAddress.

InvestToken.sol has 20 functions:

buyTokens - allow buy tokens.

sellTokens - allow sell tokens.

swapTokens - call function _mint() and mint tokens to msg.sender.

reinvest - reinvest weiAmount.

withdraw - withdrawal weiAmount.

sendDividendsToHolders - send dividends to holders if holders' balance more than minimum holders balance.

sendToGame - send tokens to gameAddress.

gameDividends - add weiAmount to casinoDividends.

price - increase priceCoeff.

mint - mints an amount of the tokens and assigns it to an account.

checkInvestTimeAndSize - check last invest time and investment limit for last 24 hours for specific account.

buyFee - check is it a first investment or not and increase investDividends by holdersWeiAmount.

sellFee - count weiAmount for sell and return it.

addDividends - increase investDividends by weiAmount.

ethereumToTokens - convert Ethereum to tokens.

tokensToEthereum - convert tokens to Ethereum.

bytesToAddress - convert bytes to address.

sqrt - return square root of given number.

deleteTokensHolder - remove tokens holder from holders.

GameWithToken contract overview

GameWithToken contract constructor sets:

callbackGas to 300000.

beneficiar to given staratBeneficiarAddress.

GameWithToken has 1 modifier:

valideAddress - check that address is valid.

GameWithToken has 24 functions:

placeBet - check that msg.value and tokensAmount enough, check that game is valid and place bet.

EthLottery – starts a lottery with ethLotteryParticipants tokensLottery – starts a lottery with tokenLotteryParticipants

sendBonusTokens – iterate through players array and distributes collected tokens depends on player’s bets balances

refundEthPrize - check that msg.sender’s waitingEthPrizes more than zero and transfer weiAmountToSend.

refundTokensPrize - check that msg.sender’s waitingTokensPrizes more than zero and transfer tokensAmountToSend.

setOraclizeGasPrice - set given gasPrice.

setOraclizeGasLimit - set given gasLimit.

setBeneficiar - set given newBeneficiar.

setInvestToken - set given investTokenAddress.

setBonusToken - set given bonusTokenAddress.

getFund - sender gets given weiAmount.

getBeneficiarFund - check that msg.sender is beneficiar and send him weiAmountToSend.

__callback – check that msg.sender is contract of oraclize. If it is callback from bet find winner and call sendWin(). Else if it is lottery choose winner from tokensHolders use random number and ranges. After that call random() till lotteryStage equal 4 and than call restartEthLottery to restart lottery.

updateEthLotteryRanges - update minEthRanges and maxEthRnages for every holder in holdersInEthLottery.

updateTokensLotteryRanges - update minTokensRanges and maxTokensRnages for every holder in holdersInTokensLottery.

validеBet - check bet for validity.

fee – calculates and returns fee amount based on constants

newQuery - add new notes to queries.

random - call function which call contract of oraclize.

sendEthWin - transfer weiAmount to winner or write weiAmount to waitingEthPrizes.

sendTokensWin - transfer tokensAmount to winner or write tokensAmount to waitingTokensPrizes.

deleteEthLotteryParticipant - removes holders from holdersInEthLottery

deleteTokensLotteryParticipant – removes holders from holdersInTokensLottery

Audit overview

Critical

No critical severity vulnerabilities were found.

High

No high severity vulnerabilities were found.

Medium

No high severity vulnerabilities were found.

Low

No low severity vulnerabilities were found.

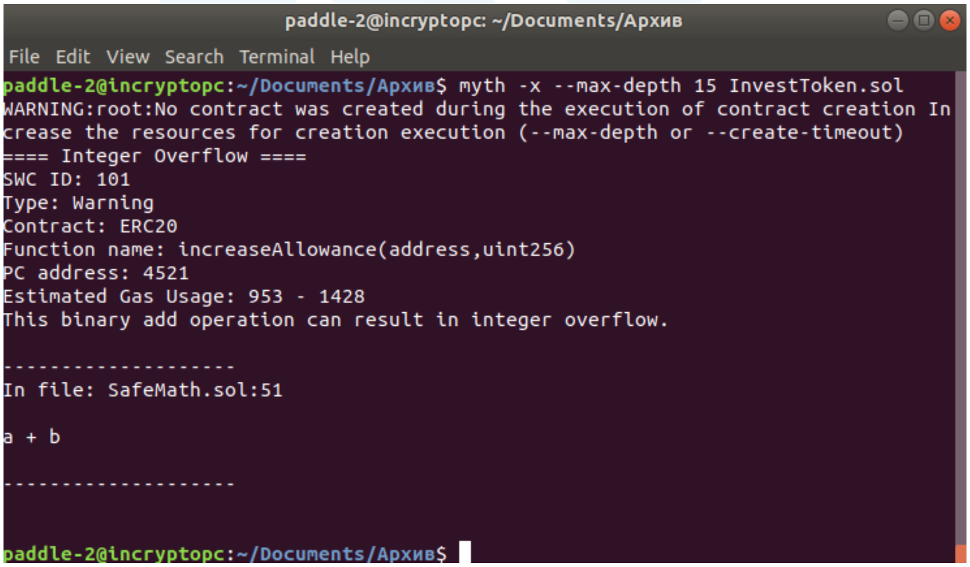
Lowest

Code style issues:

There are few code style issues (check the automated reports section)

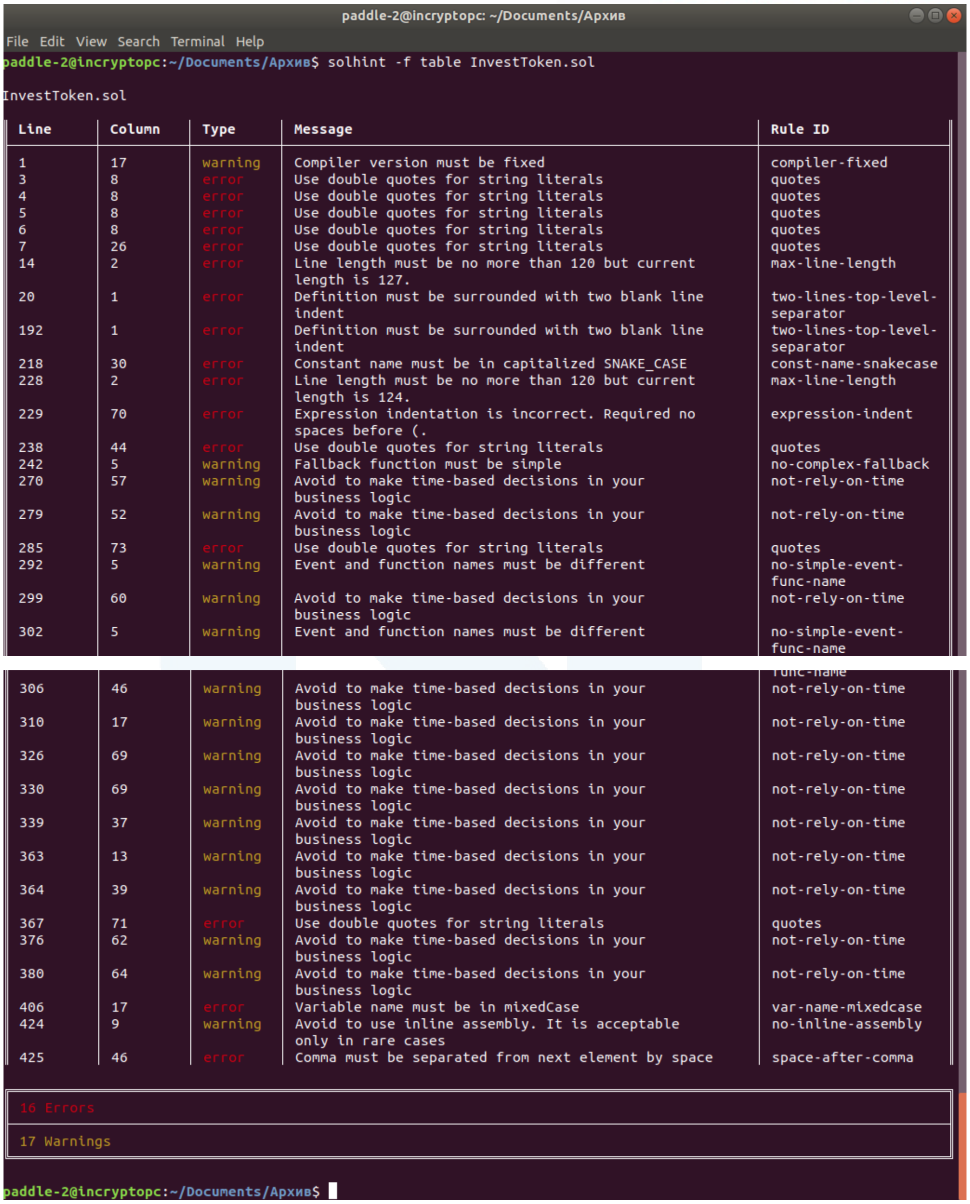
Appendix B. Automated tools reports

Myth InvestToken.sol automated report:


paddle-2@incryptopc: ~/Documents/Архив
File Edit View Search Terminal Help

```
paddle-2@incryptopc:~/Documents/Архив$ myth -x --max-depth 15 InvestToken.sol
WARNING:root:No contract was created during the execution of contract creation In
crease the resources for creation execution (--max-depth or --create-timeout)
==== Integer Overflow ====
SWC ID: 101
Type: Warning
Contract: ERC20
Function name: increaseAllowance(address,uint256)
PC address: 4521
Estimated Gas Usage: 953 - 1428
This binary add operation can result in integer overflow.

--------------------
In file: SafeMath.sol:51

a + b

--------------------


paddle-2@incryptopc:~/Documents/Архив$
```

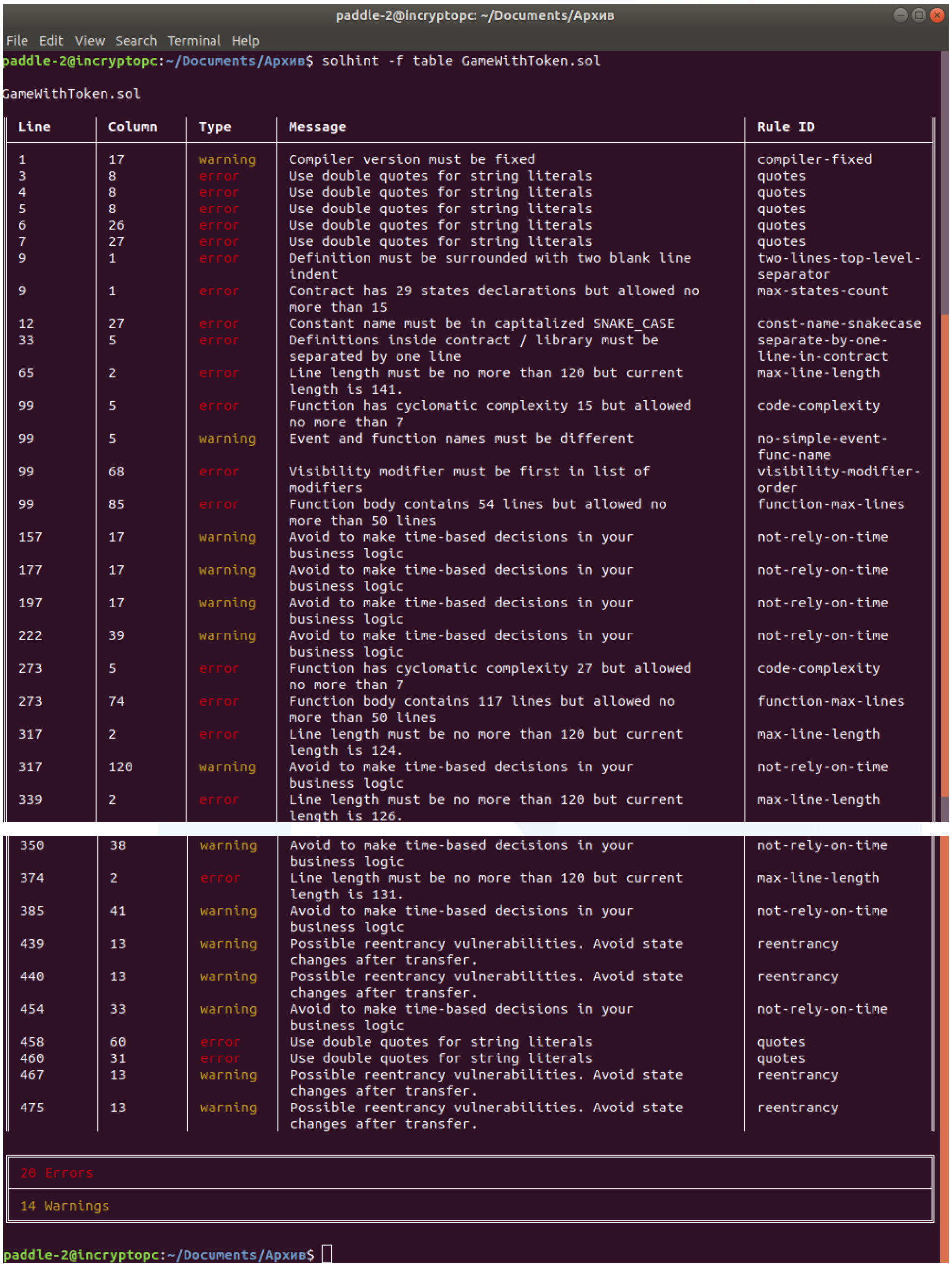
Solhint InvestToken.sol automated report:



paddle-2@incryptopc: ~/Documents/Архив
File Edit View Search Terminal Help

```
paddle-2@incryptopc:~/Documents/Архив$ solhint -f table InvestToken.sol

InvestToken.sol

 Line        Column      Type        Message                                               Rule ID

 1           17          warning     Compiler version must be fixed                        compiler-fixed
 3           8           error       Use double quotes for string literals                 quotes
 4           8           error       Use double quotes for string literals                 quotes
 5           8           error       Use double quotes for string literals                 quotes
 6           8           error       Use double quotes for string literals                 quotes
 7           26          error       Use double quotes for string literals                 quotes
 14          2           error       Line length must be no more than 120 but current      max-line-length
                                     length is 127.
 20          1           error       Definition must be surrounded with two blank line     two-lines-top-level-
                                     indent                                                separator
 192         1           error       Definition must be surrounded with two blank line     two-lines-top-level-
                                     indent                                                separator
 218         30          error       Constant name must be in capitalized SNAKE_CASE       const-name-snakecase
 228         2           error       Line length must be no more than 120 but current      max-line-length
                                     length is 124.
 229         70          error       Expression indentation is incorrect. Required no      expression-indent
                                     spaces before (.
 238         44          error       Use double quotes for string literals                 quotes
 242         5           warning     Fallback function must be simple                      no-complex-fallback
 270         57          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 279         52          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 285         73          error       Use double quotes for string literals                 quotes
 292         5           warning     Event and function names must be different            no-simple-event-
                                                                                           func-name
 299         60          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 302         5           warning     Event and function names must be different            no-simple-event-
                                                                                           func-name
 306         46          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 310         17          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 326         69          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 330         69          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 339         37          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 363         13          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 364         39          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 367         71          error       Use double quotes for string literals                 quotes
 376         62          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 380         64          warning     Avoid to make time-based decisions in your            not-rely-on-time
                                     business logic
 406         17          error       Variable name must be in mixedCase                    var-name-mixedcase
 424         9           warning     Avoid to use inline assembly. It is acceptable        no-inline-assembly
                                     only in rare cases
 425         46          error       Comma must be separated from next element by space    space-after-comma

 16 Errors

 17 Warnings

paddle-2@incryptopc:~/Documents/Архив$
```

Solhint GameWithToken.sol automated report:



paddle-2@incryptopc: ~/Documents/Архив
File Edit View Search Terminal Help

```
paddle-2@incryptopc:~/Documents/Архив$ solhint -f table GameWithToken.sol

GameWithToken.sol

 Line        Column      Type        Message                                                     Rule ID

 1           17          warning     Compiler version must be fixed                              compiler-fixed
 3           8           error       Use double quotes for string literals                       quotes
 4           8           error       Use double quotes for string literals                       quotes
 5           8           error       Use double quotes for string literals                       quotes
 6           26          error       Use double quotes for string literals                       quotes
 7           27          error       Use double quotes for string literals                       quotes
 9           1           error       Definition must be surrounded with two blank line           two-lines-top-level-
                                     indent                                                      separator
 9           1           error       Contract has 29 states declarations but allowed no          max-states-count
                                     more than 15
 12          27          error       Constant name must be in capitalized SNAKE_CASE             const-name-snakecase
 33          5           error       Definitions inside contract / library must be               separate-by-one-
                                     separated by one line                                       line-in-contract
 65          2           error       Line length must be no more than 120 but current            max-line-length
                                     length is 141.
 99          5           error       Function has cyclomatic complexity 15 but allowed           code-complexity
                                     no more than 7
 99          5           warning     Event and function names must be different                  no-simple-event-
                                                                                                 func-name
 99          68          error       Visibility modifier must be first in list of                visibility-modifier-
                                     modifiers                                                   order
 99          85          error       Function body contains 54 lines but allowed no              function-max-lines
                                     more than 50 lines
 157         17          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 177         17          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 197         17          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 222         39          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 273         5           error       Function has cyclomatic complexity 27 but allowed           code-complexity
                                     no more than 7
 273         74          error       Function body contains 117 lines but allowed no             function-max-lines
                                     more than 50 lines
 317         2           error       Line length must be no more than 120 but current            max-line-length
                                     length is 124.
 317         120         warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 339         2           error       Line length must be no more than 120 but current            max-line-length
                                     length is 126.
 350         38          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 374         2           error       Line length must be no more than 120 but current            max-line-length
                                     length is 131.
 385         41          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 439         13          warning     Possible reentrancy vulnerabilities. Avoid state            reentrancy
                                     changes after transfer.
 440         13          warning     Possible reentrancy vulnerabilities. Avoid state            reentrancy
                                     changes after transfer.
 454         33          warning     Avoid to make time-based decisions in your                  not-rely-on-time
                                     business logic
 458         60          error       Use double quotes for string literals                       quotes
 460         31          error       Use double quotes for string literals                       quotes
 467         13          warning     Possible reentrancy vulnerabilities. Avoid state            reentrancy
                                     changes after transfer.
 475         13          warning     Possible reentrancy vulnerabilities. Avoid state            reentrancy
                                     changes after transfer.


 20 Errors

 14 Warnings


paddle-2@incryptopc:~/Documents/Архив$ 
```