BINANCE
SMART CHAIN

Security Audit

MOON_STAKE

Website: https://moonstake.app

Contract:

https://bscscan.com/address/0x1888b7C11D9E156C72412A64D87Bb72B98bd0F6d#code

Haze Security

04/29/2021

CRITICAL ISSUES (critical, high severity): 0

Critical and harmful access for owners, user block ability, Bugs, and vulnerabilities that enable theft of funds, lock access to funds without possibility to restore it or lead to any other loss of funds to be transferred to any party.

ERRORS, BUGS AND WARNINGS (medium, low severity): 0

Bugs can negatively affect the usability of a program, errors that can trigger a contract failure, Lack of necessary security precautions, other warnings for owners and users, warning codes that are valid code but the compiler thinks are suspicious.

OPTIMIZATION (low severity): 1

Methods to decrease the cost of transactions in Smart-Contract.

RECOMMENDATIONS (very low severity): 0

Hint and tips to improve contract functionality and trustworthiness.

Conclusion:

In the **MOON_STAKE** Smart-Contract were found no vulnerabilities, no backdoors, and no scam scripts.

The code was tested with compatible compilers and simulate manually reviewed for all commonly known and specific vulnerabilities.

So, **MOON_STAKE** Smart-Contract is safe for use in the Binance Smart Chain main network.

Optimization suggestions

1- Loop on the dynamic variable (low severity).

If the user gets more parallel deposits his withdrawal transaction will cost more transaction fees because the loop on the dynamic variable is used in the 'withdraw' function.

In case the GAS limit exceeds the size of transaction, withdraw is not possible.

Note:

This comment is relevant only if a user creates an excessive number of parallel deposits (more than 100).

Independent description of the smart-contract functionality

The MOON_STAKE smart-contract provides the opportunity to invest any amount in BNB (from 0.05 BNB) in the contract and get 140% to 378% return on investment in 7 to 21 days if the contract balance has enough funds for payment.

- ✓ Dividends are paid from deposits of users.
- ✓ All dividends are calculated at the moment of request and available for withdrawal anytime
- ✓ Each subsequent Deposit is kept separately in the contract, in order to maintain the payment amount for each Deposit.

Launch Date: Thu Apr 29 2021 08:30:35 GMT+0000

Contract Owners Fee

Project Fee: 10% on deposit

Project Fee: 3% on auto-reinvest

THREE INVESTMENT PLANS

Plans	Total Return	Daily Profit	Days	Withdraw time
1	140%	20%	7	Any Time
2	266%	19%	14	Any Time
3	378%	18%	21	Any Time

- ❖ The minimum deposit amount is 0.05 BNB

Float Plan

Plans return are float and daily profit for a new deposit will increase by 0.5% daily

Referral System (Match Bonus)

This contract pays 8% referral commissions over 3 levels

- Level one: 5%
- Level two: 2.5%
- Level three: 0.5%

Notes:

- Referral should be an active user; it means referral address has at least one deposit

Auto Re-invest System

25% of all withdraws will be reinvested automatically.

- Users can choose the plan for new deposit on auto-reinvest

MOON_STAKE Smart-Contract Functions

- Constructor: initial plans, owner address and start date
- invest: make a new deposit
- autoReinvest: auto re-invest 25% of withdrawable amount and make a new deposit
- withdraw: transfer user profit to his wallet
- getContractBalance: return contract balance
- getPlanInfo: return plan info
- getPercent: return calculated percent
- getResult: return deposit calculated percent, profit and finish date
- getUserDividends: return user dividends
- getUserCheckpoint: return user checkpoint
- getUserReferrer: return user referrer
- getUserDownlineCount: return referral amount in three level
- getUserReferralBonus: return referral bonus
- getUserReferralTotalBonus: return total referrals
- getUserReferralWithdrawn: return total paid referrals
- getUserAvailable: return user available
- getUserAmountOfDeposits: return deposits amount
- getUserTotalDeposits: return total deposit
- getUserDepositInfo: return a deposit info
- isContract: check the address type

Disclaimer:

This audit is only to the Smart-Contract code at the specified address.

MOON_STAKE:
https://bscscan.com/address/0x1888b7C11D9E156C72412A64D87Bb72B98bd0F6d#code

Haze Security is a 3rd party auditing company who works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration is fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Haze Security.

Investors are not in any way obliged, coerced or influenced to invest in projects audited by Haze Security.

We are not responsible for your funds or guarantee you profits.

We highly recommend that investors do their own research and gain crypto experience before investing

To report any scam, malpractices and irregularities, please send a message via Telegram to @Haze013 or @Sara_Solidity for blacklisting.

Haze Security

04/29/2021

If you are interested in developing/auditing of Smart-Contracts, please contact us.

Admin: @Haze013

Auditor: @Sara_Solidity

All official info available:

Website: https://hazecrypto.net/moon_stake

Telegram Channel: t.me/HazeCrypto

Telegram Community: t.me/HazecryptoCommunity

Twitter: twitter.com/HazeCryptoTM

Instagram: instagram.com/HazeCryptoTM