polygon

Security Audit

Polyshield

Website: https://polyshield.finance

Haze Security
08/04/2021

www.hazecrypto.net

Haze Security

Contracts

Polysheild:
https://polygonscan.com/address/0xf239e69ce434c7fb408b05a0da416b14917d934e#code

MasterChef:
https://polygonscan.com/address/0x0Ec74989E6f0014D269132267cd7c5B901303306#code

PolyshieldBurner:
https://polygonscan.com/address/0xfbb307fea8cdaf614b66f82d8d233c947b07c4f5#code

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.

HIGH ISSUES (high, medium severity): 0

The owner's privileges, access and permission that cause changes in the contract results and parameters, enable/disable main modules and features, exclude/include specific users.

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): 0

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

RECOMMENDATIONS (very low severity): 1

Hint and tips to improve contract functionality and trustworthiness.

Conclusion:

In the **POLYSHIELD** 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 **POLYSHIELD** Smart-Contract is safe for use in the Polygon (Matic) main network.

RECOMMENDATIONS

1- **Owner privileges** (high, medium severity):

The owner has access to the functions:

- Add and set (update) farms
- setFeeAddress
- updateEmissionParameters
- updateEmissionRate
- updateStartBlock
- setNFTAddress
- setUSDCAddress
- setUsdcShieldLPAddress

the owner has the privilege to change some of the parameters but limits in the change range of critical variables make it safe.

Independent Description of the smart-contract functionality

The POLYSHIELD is a token deployed in the Polygon blockchain and users can earn it in LP farms and vaults.

- ❖ It is a standard ERC20 Token with a mint and burn feature. Only the Masterchef contract has the privilege of mint.
- ❖ All libraries which were used for calculation and the token in the contract are standard and safe.

Token Info (all information based on audit date)

- Total Supply: 1,000 SHI3LD
- Holders: 6 addresses
- Total Transactions: 19
- Name: PolyShield
- Symbol: SHI3LD
- Decimals: 18
- Contract: 0xf239e69ce434c7fb408b05a0da416b14917d934e

Owner/Deployer Tokens

In the first initial of the token, 1000 tokens will be transferred to the owner wallet.

Burn & Mint

The burning method is a public function that anyone can use and burn his tokens.

Mint can only call by the owner which is the Masterchef contract.

PolyshieldBurner

The contract has only one function that can be called by anyone and it burns the tokens in the contract.

Masterchef

It is a contract that controls the farms and vaults. It has the privilege of mint tokens.

- Farms can be created and updated
- Each token can only have one farm
- Users can deposit in farms
  - There is a fee in each farm that transfers a specific amount of tokens to the owner wallet. The maximum fee amount is 4%
- Users can harvest one or all farms and receive their rewards any time
- Users can increase their investment
- Users can withdraw their investments.
- On each new deposit, harvest and withdrawal, users will receive earned rewards.
- Users can force withdraw their total investment without receiving the rewards.
- Equal to 10% of all rewards will be used for NFT and burn system
  - If the NFT address set in the contract
    - Equal to 5% of rewards transfer to the NFT address (it will be set by the owner and they can use it for any reason)
    - Equal to 5% of rewards will be burnt
  - If the NFT is not set, all 10% will be burnt

Emission Rate

- If the USDC LP token is set by the owner, the emission update system activated
- The emission rate will be changed by the price of the token in the USDC
  - Less than $1, it is 100%
  - Greater than $50, it is 1%
- The min and max price can be changed by the owner to moderate the emission rate
- In the price between min and max, the emission rate will be calculated based on a curve formula

$$y = \frac{1}{curveRate}(100 - x) + \left(\frac{100}{x}\right)$$

Disclaimer:

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

POLYSHIELD:
https://polygonscan.com/address/0xf239e69ce434c7fb408b05a0da416b14917d934e#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

08/04/2021

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/polyshield

Telegram Channel: t.me/HazeCrypto

Telegram Community: t.me/HazecryptoCommunity

Twitter: twitter.com/HazeCryptoTM

Instagram: instagram.com/HazeCryptoTM

HAZE® Verified

★ VERIFIED / SAFE / AUDITED ★

HAZE CRYPTO