0x Guard

Smart contracts security assessment

Final report
Tariff: Standard

Hyper Inu (HPE)

November 2021

0xguard.com

hello@0xguard.com

Contents

⛨ Introduction

The report has been prepared for Hyper Inu (HPE) token.

Name	Hyper Inu (HPE)
Audit date	2021-11-01 - 2021-11-01
Language	Solidity
Platform	Binance Smart Chain

⛨ Contracts checked

Name	Address
Token	https://bscscan.com/address/0xe11F708A7769cB2D26cED9fd12bA54f6d07bF850

⛨ Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyse smart contracts for security vulnerabilities
- Smart contracts' logic check

🛡 Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	passed
Message call with hardcoded gas amount	passed
Typographical Error	passed
DoS With Block Gas Limit	passed
Presence of unused variables	passed
Incorrect Inheritance Order	passed
Requirement Violation	passed
Weak Sources of Randomness from Chain Attributes	passed
Shadowing State Variables	passed
Incorrect Constructor Name	passed
Block values as a proxy for time	passed
Authorization through tx.origin	passed
DoS with Failed Call	passed
Delegatecall to Untrusted Callee	passed
Use of Deprecated Solidity Functions	passed
Assert Violation	passed
State Variable Default Visibility	passed
Reentrancy	passed
Unprotected SELFDESTRUCT Instruction	passed
Unprotected Ether Withdrawal	passed
Unchecked Call Return Value	passed

Floating Pragma   passed

Outdated Compiler Version   passed

Integer Overflow and Underflow   passed

Function Default Visibility   passed

Classification of issue severity

High severity   High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.

Medium severity   Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.

Low severity   Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Lack of increaseAllowance and decreaseAllowance functions (Token)

There is a known frontrun [attack on approve/transferFrom methods](#).

Recommendation: We recommend adding increaseAllowance and decreaseAllowance functions to atomically change allowance.

2. Decimals use uint256 instead of uint8 (Token)

[ERC20](#) and [BEP20](#) standard require decimals() function to return uint8, but token returns uint256.

Conclusion

Hyper Inu (HPE) Token contract was audited. 2 low severity issues were found.

🛡 Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability)set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

🛡 Slither check output

INFO:Detectors:

transfer(address,uint256) should be declared external:

    - Token.transfer(address,uint256) (contracts/Token.sol#31-37)

transferFrom(address,address,uint256) should be declared external:

    - Token.transferFrom(address,address,uint256) (contracts/Token.sol#39-47)

approve(address,uint256) should be declared external:

    - Token.approve(address,uint256) (contracts/Token.sol#49-53)

allowance(address,address) should be declared external:

    - Token.allowance(address,address) (contracts/Token.sol#55-57)

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external

INFO:Slither:contracts/Token.sol analyzed (1 contracts with 75 detectors), 6 result(s) found

INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration

0x Guard