AstraSec

Hyperpie
Security Audit Report

March 22, 2025

Contents

1 Introduction

1.1 About Hyperpie

Hyperpie is an advanced liquid staking platform tailored for Hyperliquid users, allowing them to stake HYPE tokens while preserving asset flexibility. It employs a sophisticated staking mechanism wherein users deposit HYPE tokens and receive mHYPE tokens in return. The exchange rate between HYPE and mHYPE is dynamically adjusted via a price provider system, which incorporates rate change limits and defined update windows to safeguard against manipulation.

1.2 Source Code

The following source code was reviewed during the audit:

- https://github.com/magpiexyz/hyperpie/tree/feat/hype-lst-staking
- CommitID: ba87f502f42df10a9275435a36ae78e6da61c2cf

And this is the final version representing all fixes implemented for the issues identified in the audit:

- https://github.com/magpiexyz/hyperpie/
- CommitID: 3a0891c58890832b9b0c723ae52728fea576fab2

1.3 Revision History

Version	Date	Description
v1.0	March 7, 2025	Initial Audit
v1.1	March 22, 2025	Latest main commitID

2 Overall Assessment

This report has been compiled to identify issues and vulnerabilities within the Hyperpie protocol. Throughout this audit, we identified a total of 4 issues spanning various severity levels. By employing auxiliary tool techniques to supplement our thorough manual code review, we have discovered the following findings.

Severity	Count	Acknowledged	Won't Do	Addressed
Critical	–	–	–	–
High	–	–	–	–
Medium	2	1	–	1
Low	2	–	–	2
Informational	–	–	–	–
Total	4	1	–	3

3 Vulnerability Summary

3.1 Overview

Click on an issue to jump to it, or scroll down to see them all.

3.2 Security Level Reference

In web3 smart contract audits, vulnerabilities are typically classified into different severity levels based on the potential impact they can have on the security and functionality of the contract. Here are the definitions for critical-severity, high-severity, medium-severity, and low-severity vulnerabilities:

Severity	Acknowledged
C-X (Critical)	A severe security flaw with immediate and significant negative consequences. It poses high risks, such as unauthorized access, financial losses, or complete disruption of functionality. Requires immediate attention and remediation.
H-X (High)	Significant security issues that can lead to substantial risks. Although not as severe as critical vulnerabilities, they can still result in unauthorized access, manipulation of contract state, or financial losses. Prompt remediation is necessary.
M-X (Medium)	Moderately impactful security weaknesses that require attention and re-mediation. They may lead to limited unauthorized access, minor financial losses, or potential disruptions to functionality.
L-X (Low)	Minor security issues with limited impact. While they may not pose significant risks, it is still recommended to address them to maintain a robust and secure smart contract.
I-X (Informational)	Warnings and things to keep in mind when operating the protocol. No immediate action required.
U-X (Undetermined)	Identified security flaw requiring further investigation. Severity and impact need to be determined. Additional assessment and analysis are necessary.

3.3 Vulnerability Details

3.3.1 [M-1] Sandwich Attack on updateHyperpiePrice()

TARGET	CATEGORY	IMPACT	LIKELIHOOD	STATUS
PriceProvider.sol	Business Logic	Medium	Low	Mitigated

The *_updatemHypePrice()* function, which allows a price oracle to periodically update the *hHYPE/HYPE* exchange rate, is susceptible to a sandwich attack. This vulnerability stems from the fact that staked *HYPE* within Hyperpie is used for staking on Hyperliquid L1, and the rewards generated from this staking activity generally cause the hHYPE/HYPE exchange rate to gradually increase over time. A malicious actor can exploit this predictable price increase by strategically inserting transactions immediately before and after the oracle's call to _updatemHypePrice() within the same block. The attack sequence is as follows:

- Stake *HYPE*: The attacker stakes *HYPE* into Hyperpie just before the *_updatemHypePrice()* function is called.
- Oracle Update: The price oracle calls *_updatemHypePrice()* to update the *hHYPE/HYPE* exchange rate.
- Withdraw *HYPE*: The attacker immediately withdraws their staked HYPE after the update.

As a direct result of the increased exchange rate, the attacker receives more *HYPE* upon withdrawal than they would have received before the update. This excess *HYPE* effectively comes from the staking rewards that should be distributed among other stakers.

hyperpie - PriceProvider.sol

```
66  function _updatemHypePrice(uint256 exchangeRate) internal {
67      address mHYPE = hyperpieConfig.getAddress(HyperpieConstants.MHYPE_TOKEN);
68      ImHYPE(mHYPE).updateExchangeRateToUnderlying(exchangeRate);
69      emit ExchangeRateUpdate(HyperpieConstants.PLATFORM_TOKEN_ADDRESS, mHYPE, exchangeRate);
70  }
```

Remediation To mitigate the issue, it is recommended that the newly updated exchange rate from *_updatemHypePrice()* only takes effect starting from the subsequent block. This delay would prevent attackers from sandwiching the *_updatemHypePrice()* transaction with their stake and unstake transactions within the same block, effectively neutralizing the exploit.

3.3.2 [M-2] Potential Risks Associated with Centralization

TARGET	CATEGORY	IMPACT	LIKELIHOOD	STATUS
Multiple Contracts	Security	High	Low	Acknowledged

The Hyperpie protocol relies on multiple privileged accounts that possess extensive control over critical operations, introducing notable centralization risks. These accounts, assigned distinct roles, can unilaterally influence the protocol's functionality and integrity. Below are key examples of privileged functions and their associated roles:

- Admin Role: Can grant additional privileged roles, configure essential protocol parameters, and withdraw all *HYPE* tokens from the protocol.
- Oracle Role: Controls the exchange rate between *mHYPE* and *HYPE*, directly impacting token economics.
- Minter Role: Authorized to mint *hHYPE* tokens, affecting token supply.
- Burner Role: Permitted to burn *hHYPE* tokens, influencing circulating supply.

This concentration of power in privileged accounts creates a dependency on their security and trustworthiness.

hyperpie - HyperpieWithdrawManager.sol

```
350  function emergencyWithdraw(uint256 amount, address recipient) external onlyDefaultAdmin {
351      if (recipient == address(0)) revert InvalidDestination();
352      (bool success,) = payable(recipient).call{ value: amount }("");
353      if (!success) revert TransferFailed();
354      emit EmergencyWithdraw(amount, recipient);
355  }
```

Remediation To mitigate the identified issue, it is recommended to introduce multi-sig mechanism to undertake the role of the privileged accounts. Moreover, it is advisable to implement timelocks to govern all modifications to the privileged operations.

Response By Team This issue has been acknowledged by the team.

3.3.3 [L-1] Emission of UpdatedHyperpieConfig() Event in initialize()

TARGET	CATEGORY	IMPACT	LIKELIHOOD	STATUS
Multiple Contracts	Coding Practices	Low	Low	Addressed

The Hyperpie protocol defines an *UpdatedHyperpieConfig()* event to log changes to the *hyperpieConfig* state variable, promoting transparency and auditability of configuration updates. However, this event is not emitted in the *initialize()* functions of the PriceProvider and HyperpieWithdrawManager contracts.

The omission of *UpdatedHyperpieConfig()* events in these initialization functions diminishes the protocol's transparency and auditability. Off-chain systems or external monitors depending on these events to track *hyperpieConfig* updates may miss or fail to verify configuration changes during initialization, which could result in inconsistencies or undetected misconfigurations.

hyperpie - PriceProvider.sol

```
26  function initialize(address hyperpieConfigAddr) external initializer    {
27      UtilLib.checkNonZeroAddress(hyperpieConfigAddr);
28
29      hyperpieConfig = IHyperpieConfig(hyperpieConfigAddr);
30
31      rateIncreaseLimit = 100; // 1% limit
32      rateChangeWindowLimit = 2 hours;
33  }
```

Remediation Ensure the *UpdatedHyperpieConfig()* event is emitted after successfully setting the *hyperpieConfig* state variable in the *initialize()* functions of both the PriceProvider and HyperpieWithdrawManager contracts.

3.3.4 [L-2] Inconsistent Role Usage in mHYPE::pause()

TARGET	CATEGORY	IMPACT	LIKELIHOOD	STATUS
mHYPE.sol	Coding Practices	Low	Low	Addressed

The mHYPE contract employs a *Manager* role to control the *pause()* function, enabling the pausing of contract operations. However, other contracts within the Hyperpie ecosystem, such as the HyperpieStaking contract, utilize a *Pauser* role for the same purpose. This inconsistency in role design, as shown in the provided code snippet, may introduce unnecessary complexity and management challenges for protocol governance and access control.

Specifically, the *mHYPE::pause()* function is restricted by the *onlyHyperpieManager* modifier, whereas a standardized *onlyPauser* modifier is used in other contracts for pausing functionality.

hyperpie - mHYPE.sol

```
103  function pause() external onlyHyperpieManager {
104      _pause();
105  }
```

hyperpie - HyperpieStaking.sol

```
130  function pause() external onlyPauser {
131      _pause();
132  }
```

Remediation Refactor the mHYPE contract to align with the ecosystem's standard by replacing the *onlyHyperpieManager* modifier with the *onlyPauser* modifier for the *pause()* function.

4 Appendix

4.1 About AstraSec

AstraSec is a blockchain security company that serves to provide high-quality auditing services for blockchain-based protocols. With a team of blockchain specialists, AstraSec maintains a strong commitment to excellence and client satisfaction. The audit team members have extensive audit experience for various famous DeFi projects. AstraSec's comprehensive approach and deep blockchain understanding make it a trusted partner for the clients.

4.2 Disclaimer

The information provided in this audit report is for reference only and does not constitute any legal, financial, or investment advice. Any views, suggestions, or conclusions in the audit report are based on the limited information and conditions obtained during the audit process and may be subject to unknown risks and uncertainties. While we make every effort to ensure the accuracy and completeness of the audit report, we are not responsible for any errors or omissions in the report.

We recommend users to carefully consider the information in the audit report based on their own independent judgment and professional advice before making any decisions. We are not responsible for the consequences of the use of the audit report, including but not limited to any losses or damages resulting from reliance on the audit report.

This audit report is for reference only and should not be considered a substitute for legal documents or contracts.

4.3 Contact

Phone	+86 156 0639 2692
Email	contact@astrasec.ai
Twitter	https://twitter.com/AstraSecAI