

Horus Group

Hadron Finance

Security Assessment

November 5th 2022



For: Hadron Finance

By: **Horus Group** - Thomas

Horus Group

horusgroup.org

team.horus.group@gmail.com

Disclaimer

This audit report is not an endorsement of any protocol and does not represent the opinion of the protocol in any way. This report does not guarantee that the protocol under consideration is risk-free or provide any indication of economic value or legal compliance.

Horus Group does not provide a warranty towards anyone using the particular protocol, but represents an extensive auditing process meant to increase the quality of code and reduce possible vulnerabilities found within the scope of the review.

Horus Group's goal is to reduce attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology that has been analyzed.

The scope of the analysis conducted by the group is strictly limited to the code provided by the client, and not linked to any parameters that are set upon deployment.

Hadron Finance engaged The Horus Group for a comprehensive audit on its core protocol. The formal audit began on November 2nd, 2022 and lasted to November 5th, 2022. Due to the low degree of differentials within the contracts and the [previously audited Cream codebase](#), the major focus of the audit report was the custom oracle from Aداستريا and interactions with the Comptroller.

Details about the project, potential vulnerabilities, and coverage discovered can be found in this report

Horus Group

Protocol Summary:

Protocol	Hadron Finance
Description	The Hadron codebase covered in this audit is focused on the Adrastia Oracle and the core libraries.
Platform	Evmos; Solidity
Codebase	Github Repository
Commits	90a6532cdef5834c6bbe017fbe128a3b26940a9f

Vulnerability Summary:

Total Issues	3
Total Critical	0
Total Major	0
Total Moderate	0
Total Minor	1
Total Informational	2

Horus Group

Overall Summary:

The report represents a formal audit on the smart contracts behind Hadron Finance, a Cream fork deployed on Evmos.

The issues identified below pose no threat to the security of the contracts. The findings mostly represent procedural and documentation issues classified as informational flaws.

Files In Scope:

ID	Contract	Location
CP	Comptroller.sol	contracts/comptroller.sol
AP	AdrastiaPriceOracle.sol	contracts/AdrastiaPriceOracle.sol
CS	ComptrollerStorage.sol	contracts/ComptrollerStorage.sol

Findings:

ID	Type	Severity
AP-01	Documentation	Informational
AP-02	Gas Optimization	Informational
CP-01	Flaw	Minor

Horus Group

VULNERABILITIES & FUNCTIONAL ISSUES

ID	CATEGORY	LOCATION	STATUS
AP-01	Informational	AdrastiaPriceOracle.sol	ACKNOWLEDGED
<p>Description:</p> <p>setOracleAddress fails to follow SPDX Guidelines.</p>			
<p>Problem:</p> <pre>function setOracleAddress(address aggregated, address usdPeggedAggregated) public onlyOwner { require(aggregated != address(0), "Aggregated addr not set"); require(usdPeggedAggregated != address(0), "usdPeggedAggregated addr not set"); aggregatedOracle = aggregated; usdPeggedAggregatedOracle = usdPeggedAggregated; }</pre>			
<p>Recommendation:</p> <p>In line with best practices, every function should be documented via SPDX.</p>			

ID	CATEGORY	LOCATION	STATUS
AP-02	Informational	AdrastiaPriceOracle.sol	ACKNOWLEDGED
<p>Description:</p> <p>Custom errors should be used in line with the rest of the codebase.</p>			
<p>Problem:</p> <pre>require(aggregated != address(0), "Aggregated addr not set"); require(usdPeggedAggregated != address(0), "usdPeggedAggregated addr not set");</pre>			

Horus Group

Recommendation:

In order to keep code consistency, custom errors should be used in lieu of string based errors. This change would save 76 gas from the current implementation.

ID	CATEGORY	LOCATION	STATUS
CP-01	Minor	Comptroller.sol	ACKNOWLEDGED

Description:

The lack of a secondary oracle means that an issue underlying the Aداستريا Price Oracle could affect the solvency of the market. Although Aداستريا itself has taken precautions, this should be taken into account.

Problem:

```
vars.sumBorrowPlusEffects = mul_ScalarTruncateAddUInt(  
    vars.oraclePrice,  
    borrowAmount,
```

Recommendation:

Add a backup oracle given divergence of greater than 5% between primary and secondary oracle.