ChainLight

Hyperlane PR #5752, #5757 Security Audit

: Hyperlane PR #5752, #5757

Apr 18, 2025

Revision 1.0

ChainLight@Theori

Table of Contents

Executive Summary

From **01 April 2025**, ChainLight (Theori) conducted a security audit of Hyperlane PRs #5752 and #5757, which introduced smart-contract changes. The engagement focused on uncovering critical vulnerabilities and assessing their potential impact.

Summary of Findings

- **Medium:** 1

Audit Overview

Scope

Name	Hyperlane PR #5752, #5757 Security Audit
Target / Version	• Git Repository (`hyperlane-xyz/hyperlane-monorepo`): PR `#5752` (commit `9156292fe61798a8463f47323efe70a6a6cec66e`), PR `#5757` (commit `26f78da2ded95d6d0f6e95b9f9fae2ac90bdfe53`)
Application Type	Smart contracts
Lang. / Platforms	Smart contracts [Solidity]

Code Revision

N/A

Severity Categories

Severity	Description
Critical	The attack cost is low (not requiring much time or effort to succeed in the actual attack), and the vulnerability causes a high-impact issue. (e.g., Effect on service availability, Attacker taking financial gain)
High	An attacker can succeed in an attack which clearly causes problems in the service's operation. Even when the attack cost is high, the severity of the issue is considered "high" if the impact of the attack is remarkably high.
Medium	An attacker may perform an unintended action in the service, and the action may impact service operation. However, there are some restrictions for the actual attack to succeed.
Low	An attacker can perform an unintended action in the service, but the action does not cause significant impact or the success rate of the attack is remarkably low.
Informational	Any informational findings that do not directly impact the user or the protocol.
Note	Neutral information about the target that is not directly related to the project's safety and security.

Status Categories

Status	Description
Reported	ChainLight reported the issue to the client.
WIP	The client is working on the patch.
Patched	The client fully resolved the issue by patching the root cause.
Mitigated	The client resolved the issue by reducing the risk to an acceptable level by introducing mitigations.
Acknowledged	The client acknowledged the potential risk, but they will resolve it later.
Won't Fix	The client acknowledged the potential risk, but they decided to accept the risk.

Finding Breakdown by Severity

Category	Count	Findings
Critical	0	• N/A
High	0	• N/A
Medium	1	• `HYPERLANE-2504-1-001`
Low	0	• N/A
Informational	0	• N/A
Note	0	• N/A

Findings

Summary

#	ID	Title	Severity	Status
1	HYPERLANE-2504-1-001	Usage of Shares in Allowance Accounting of HypERC4626 May Be Problematic	Medium	Patched

#1 `HYPERLANE-2504-1-001` Usage of Shares in Allowance Accounting of `HypERC4626` May Be Problematic

ID	Summary	Severity
`HYPERLANE-2504-1-001`	`HypERC4626` records allowances in **shares** while its public interface operates in **asset units**. Because each share represents more assets as the `exchangeRate` rises, the asset amount of a previously granted allowance grows automatically after a rebase. As a result, a spender can transfer more assets than the token holder may have originally intended.	Medium

Description

`HypERC4626` converts the asset amount supplied by the user into shares (`assetsToShares`) when managing the allowance. When the `exchangeRate` (the value of a share) rises before `transferFrom`, the stored shares translate to a larger asset value, so the effective allowance increases.

For example:

1. Alice approves Bob for 100 assets when 1 share equals 1 asset. This is stored as an allowance of 100 shares.
2. The rate changes so that 1 share equals 2 assets.
3. Bob can now call `transferFrom` for 200 assets because the 100 shares granted to him are now worth 200 assets.

This may be the intended behavior; however, it can be unintuitive for users and integrators because it does not match existing, well-known implementations of rebasing tokens. Comparing implementations:

- **Lido stETH** – Users approve and transfer in *assets*; the contract converts to shares internally **but not for allowances (it still records allowances in assets).** Share-denominated functions exist separately.

- **OpenZeppelin ERC4626** – Users approve and transfer in *shares*; storage and allowances are also in shares.
- **HypERC4626** – Users approve and transfer in *assets*; the contract converts to shares internally **and stores allowances in shares**.

Impact

Medium

A malicious or unsuspecting spender may move more assets than permitted, potentially draining a user's entire rebase gain.

We assign lower severity than we normally would because rebasing is expected to be very infrequent. Although an attacker could theoretically trigger a rebase by donating to the underlying vault, the impact would likely be negligible compared with the attacker's cost.

Recommendation

Either document this behavior clearly with an explicit warning, or update the allowance interfaces to align with a well-known implementation.

Remediation

Patched

The change to allowance accounting has been reverted, so it is now accounted in assets.

Revision History

Version	Date	Description
1.0	Apr 18, 2025	Initial version

Theori, Inc. (“We”) is acting solely for the client and is not responsible to any other party. Deliverables are valid for and should be used solely in connection with the purpose for which they were prepared as set out in our engagement agreement. You should not refer to or use our name or advice for any other purpose. The information (where appropriate) has not been verified. No representation or warranty is given as to accuracy, completeness or correctness of information in the Deliverables, any document, or any other information made available. Deliverables are for the internal use of the client and may not be used or relied upon by any person or entity other than the client. Deliverables are confidential and are not to be provided, without our authorization (preferably written), to entities or representatives of entities (including employees) that are not the client, including affiliates or representatives of affiliates of the client.