

Alpha Vault 0.3.2

Smart Contract Security Assessment

November 2024

Prepared for:

Meteora

Prepared by:

Offside Labs

Sirius Xie

Ronny Xing





Contents

1	About Offside Labs	2
2	Executive Summary	3
3	Summary of Findings	4
4	Key Findings and Recommendations	5
4.1	Informational and Undetermined Issues	5
5	Disclaimer	6



1 About Offside Labs

Offside Labs is a leading security research team, composed of top talented hackers from both academia and industry.

We possess a wide range of expertise in modern software systems, including, but not limited to, *browsers*, *operating systems*, *IoT devices*, and *hypervisors*. We are also at the forefront of innovative areas like *cryptocurrencies* and *blockchain technologies*. Among our notable accomplishments are remote jailbreaks of devices such as the **iPhone** and **PlayStation 4**, and addressing critical vulnerabilities in the **Tron Network**.

Our team actively engages with and contributes to the security community. Having won and also co-organized *DEFCON CTF*, the most famous CTF competition in the Web2 era, we also triumphed in the **Paradigm CTF 2023** within the Web3 space. In addition, our efforts in responsibly disclosing numerous vulnerabilities to leading tech companies, such as *Apple*, *Google*, and *Microsoft*, have protected digital assets valued at over **\$300 million**.

In the transition towards Web3, Offside Labs has achieved remarkable success. We have earned over **\$9 million** in bug bounties, and **three** of our innovative techniques were recognized among the **top 10 blockchain hacking techniques of 2022** by the Web3 security community.



<https://offside.io/>



<https://github.com/offsidelabs>



https://twitter.com/offside_labs



2 Executive Summary

Introduction

Offside Labs completed a security audit of *Alpha Vault* smart contracts, starting on Nov 12, 2024, and concluding on Nov 15, 2024.

Project Overview

This update primarily expands the flexibility in creating and configuring *Alpha Vault* related vaults and pools in *DLMM* and *Dynamic AMM*.

Alpha Vault supports three modes, *Permissionless*, *PermissionWithMerkleProof* and *PermissionWithAuthority*, for creating escrow.

Audit Scope

The assessment scope contains mainly the smart contracts of the alpha-vault program for the *Alpha Vault* project.

The audit is based on the following specific branches and commit hashes of the codebase repositories:

- Alpha Vault
 - Codebase: <https://github.com/MeteoraAg/alpha-vault>
 - Commit Hash: 8e59e09e134f0aca9455c760c8afa791795f2abd
 - Branch: feat/support-non-backend-whitelist

We listed the files we have audited below:

- Alpha Vault PR-64

Findings

The security audit revealed:

- 0 critical issue
- 0 high issues
- 0 medium issues
- 0 low issues
- 1 informational issues

Further details, including the nature of these issues and recommendations for their remediation, are detailed in the subsequent sections of this report.



3 Summary of Findings

ID	Title	Severity	Status
01	Incorrect Duration Constants in Alpha Vault	Informational	Fixed



4 Key Findings and Recommendations

4.1 Informational and Undetermined Issues

Incorrect Duration Constants in Alpha Vault

Severity: Informational

Status: Fixed

Target: Smart Contract

Category: Math

The definitions of the following constants in Alpha Vault are inconsistent with the comments.

```
15 #[cfg(not(feature = "localnet"))]
16 pub const MAX_LOCK_SLOT_DURATION: u64 = SLOT_BUFFER * 3 * 365; // 1 year
17 #[cfg(not(feature = "localnet"))]
18 pub const MAX_LOCK_TIME_DURATION: u64 = TIME_BUFFER * 3 * 365; // 1 year
19 #[cfg(not(feature = "localnet"))]
20 pub const MAX_VESTING_SLOT_DURATION: u64 = SLOT_BUFFER * 3 * 365; // 1
   ↳ year
21 #[cfg(not(feature = "localnet"))]
22 pub const MAX_VESTING_TIME_DURATION: u64 = TIME_BUFFER * 3 * 365; // 1
   ↳ year
```

[programs/alpha-vault/src/constants.rs#L15-L31](#)

In the formulas, the `SLOT_BUFFER` and `TIME_BUFFER` correspond to 20 minutes in real time, while the values calculated for the four Duration constants correspond to 365 hours in actual time, not 365 days in a year.

Each of these four constants needs to be multiplied by 24 .



5 Disclaimer

This audit report is provided for informational purposes only and is not intended to be used as investment advice. While we strive to thoroughly review and analyze the smart contracts in question, we must clarify that our services do not encompass an exhaustive security examination. Our audit aims to identify potential security vulnerabilities to the best of our ability, but it does not serve as a guarantee that the smart contracts are completely free from security risks.

We expressly disclaim any liability for any losses or damages arising from the use of this report or from any security breaches that may occur in the future. We also recommend that our clients engage in multiple independent audits and establish a public bug bounty program as additional measures to bolster the security of their smart contracts.

It is important to note that the scope of our audit is limited to the areas outlined within our engagement and does not include every possible risk or vulnerability. Continuous security practices, including regular audits and monitoring, are essential for maintaining the security of smart contracts over time.

Please note: we are not liable for any security issues stemming from developer errors or misconfigurations at the time of contract deployment; we do not assume responsibility for any centralized governance risks within the project; we are not accountable for any impact on the project's security or availability due to significant damage to the underlying blockchain infrastructure.

By using this report, the client acknowledges the inherent limitations of the audit process and agrees that our firm shall not be held liable for any incidents that may occur subsequent to our engagement.

This report is considered null and void if the report (or any portion thereof) is altered in any manner.



 <https://offside.io/>

 <https://github.com/offsidelabs>

 https://twitter.com/offside_labs