Zellic

Valorem Options

Smart Contract Patch Review

August 29, 2023

Prepared for:

Valorem Labs

Prepared by:

Katerina Belotskaia

Zellic Inc.

About Zellic

Zellic was founded in 2020 by a team of blockchain specialists with more than a decade of combined industry experience. We are leading experts in smart contracts and Web3 development, cryptography, web security, and reverse engineering. Before Zellic, we founded perfect blue, the top competitive hacking team in the world. Since then, our team has won countless cybersecurity contests and blockchain security events.

Zellic aims to treat clients on a case-by-case basis and to consider their individual, unique concerns and business needs. Our goal is to see the long-term success of our partners rather than to simply provide a list of present security issues. Similarly, we strive to adapt to our partners' timelines and to be as available as possible. To keep up with our latest endeavors and research, check out our website zellic.io or follow @zellic_io on Twitter. If you are interested in partnering with Zellic, please email us at hello@zellic.io or contact us on Telegram at https://t.me/zellic_io.

1 Introduction

We were asked to review a minor patch to Valorem Options which decreased the expiry window from 1 day to 1 hour and increased the protocol fee from 5 to 15 basis points.

1.1 Scope

The engagement involved a review of the following targets:

Valorem Options

Repository	https://github.com/valorem-labs-inc/clear
Versions	`fe39eb73c5354bdebcc5cc61031a9585c2fe0c25`
Programs	• ValoremOptionsClearinghouse.sol
Type	Solidity
Platform	EVM-compatible

Contact Information

The following consultants were engaged to conduct the assessment:

Katerina Belotskaia, Security Engineer
kate@zellic.io

1.2 Disclaimer

This assessment does not provide any warranties about finding all possible issues within its scope; in other words, the evaluation results do not guarantee the absence of any subsequent issues. Zellic, of course, also cannot make guarantees about any additional code added to the assessed project after the audit version of our assessment. Furthermore, because a single assessment can never be considered comprehensive, we always recommend multiple independent assessments paired with a bug bounty program.

For each finding, Zellic provides a recommended solution. All code in these recommendations are intended to convey how an issue may be resolved (i.e., the idea), but

they may not be tested or functional code.

Finally, the contents of this assessment report are for informational purposes only; do not construe any information in this report as legal, tax, investment, or financial advice. Nothing contained in this report constitutes a solicitation or endorsement of a project by Zellic.

2 Smart Contract Patch Review

Commit fe39eb73 introduced changes to the expiry window and protocol fee. After conducting a comprehensive review, we have determined that these changes do not raise any security concerns. A summary of the changes is provided below.

2.1 Decrease expiry window

The minimum expiry window, the time during which an option type is eligible for exercise, was decreased from 1 day to 1 hour.

Previously, a 1-day expiry window was associated to the lifetime of a bucket, where all daily options were consolidated within a single bucket. Subsequently, a new bucket was created on the following day. However, revisions were made to this approach in order to address an issue, which, due to the way the option baskets are organized (by day), allowed participants to predict that if a specific `exercise` occurs in today's basket, then writing to it will lead to a guaranteed share of exercise tokens.

Presently, if the last bucket is assigned exercise, a new bucket is generated. As a result of this modification, the bucket creation process is no longer time-dependent which enables the reduction of the expiry window.

2.2 Increase protocol fee

A change was made to the protocol fee value, the `feeBps` was increased from 5 to 15 basis points.