DECENTRALIZED INTELLIGENCE

Vulnerability Report

Produced for

Aurigami Protocol

Please contact us immediately.

Introduction

The Aurigami Protocol, a DeFi Lending Protocol forked from Compound V2, has recently onboarded the Aurora chain. However, our AI-enhanced security analysis tool has identified a critical vulnerability in the protocol's implementation on the Aurora chain.

This vulnerability leaves the assets on the Aurora chain exposed to potential exploitation by malicious attackers. If left unaddressed, this security flaw could lead to the unauthorized extraction of funds, putting users' investments at risk. Urgent action is required to mitigate this threat and ensure the safety of the assets held within the Aurigami Protocol on the Aurora chain.

Background

Compound V2, as a commonly known DeFi lending protocol, has been forked by various teams. However, inside its codebase, a critical bug was found regarding rounding errors on empty market initalization. Specifically, In the `mintFresh` function, the `exchangeRateStoredInternal` function calculates the exchange rate by dividing the current pool assets (including balances, lent assets, and subtracting returned assets) by the total shares. If a hacker injects the smallest unit of a share when the pool is first created or emptied, and then transfers a certain amount of funds directly into the pool, this will result in an extremely large net value according to the above calculation. Besides, the `redeemUnderlying` function provides the user the interface to withdraw a certain **amount of underlying tokens**. A hacker can do as the followings to exploit this vulnerability:

1. The attacker can inject 2 shares of the smallest unit. (2 wei of `cToken`)
2. The attack transfers a large number of tokens into the pool.
3. The attacker borrows assets from the remaining markets.
4. The attacker calls `redeemUnderlying` to redeem all except 1 wei of underlying assets. In calculation, this will result in burning 1 wei of cToken (share) and the other 1 wei of share is still counted as very valuable due to step 2. So the attacker is still insolvency but able to redeem all but 1 wei of underlying assets.
5. The attacker can liquidate the previous attack contract and perform again until draining of the whole market.

There are several previous attacks that happened among various Compound V2 forks, as listed below.

- Hundred Finance Attack.

- Onyx attack.

Aurigami Protocol Case

In the Protocol Case, the empty markets are:

- **auUSDCNative Market**: 0x10D56d6E5968016dF5930E8Ce50d2d08EC59774c
- **auUSDTNative Market**: 0xdDfd0407220026c6566979B5be6A4983d1247a3E

Further, the following markets are in danger of being drained (stolen of all funds available):

- **auUSDC Market**: 0x4f0d864b1ABf4B701799a0b30b57A22dFEB5917b
- **auETH Market**: 0xca9511B610bA5fc7E311FDeF9cE16050eE4449E9
- **auWBTC Market**: 0xCFb6b0498cb7555e7e21502E0F449bf28760Adbb
- **auUSDT Market**: 0xaD5A2437Ff55ed7A8Cad3b797b3eC7c5a19B1c54
- **auWNEAR Market**: 0xaE4fac24dCdAE0132C6d04f564dCf059616E9423
- **auSTNEAR Market**: 0x3195949f267702723bc614cAE037cdc8D1E94786
- **auUSDCNative Market**: 0x10D56d6E5968016dF5930E8Ce50d2d08EC59774c
- **auUSDTNative Market**: 0xdDfd0407220026c6566979B5be6A4983d1247a3E

Our Request

We found a bug bounty program on your website (https://docs.aurigami.finance/public/resources/bug-bounty). We believe this is a critical bug and would appreciate it if we can receive the bug bounty. We would be delighted to further assist you with an audit; please do not hesitate to reach out to us.

We would very much appreciate a shoutout on X (https://twitter.com/d23e_AG), where you can ideally share that we helped secure your protocol given our AI-enhanced security analysis tool. We would further appreciate it if we can reference your protocol on our list of projects we helped to secure.

Conlusion and Disclaimer

This report was created on: April 16, 2024. We hope you find this report informative and useful. If you have any questions or need further clarification, please do not hesitate to contact us at contact@d23e.ch.

The report is provided solely for informational purposes and should not be considered as an endorsement, recommendation, or any form of legal, financial, or investment advice.

The report is based on the code at the time and does not account for any updates, modifications, or alterations to the code that may occur after the report date. The code was assessed "as-is" and the findings represent the state of the code at the time of the assessment.

Although every reasonable effort has been made to ensure the accuracy, completeness, and fairness of the report and findings contained within the report, it is provided on an "as-is" basis without any warranties, representations, or guarantees of any kind, express or implied. This includes, but is not limited to, warranties of merchantability, fitness for a particular purpose, non-infringement, accuracy, or the presence or absence of errors, whether or not discoverable.

The authors, evaluators, and any associated parties disclaim all liability for any losses, damages, costs, or expenses (including legal fees) arising directly or indirectly from the use of or reliance on the report or its findings. This includes, but is not limited to, any damage or loss caused by errors, omissions, inaccuracies, or any misleading or out-of-date information.

The reader is solely responsible for any actions or decisions taken based on the information provided in this report. It is highly recommended that, where necessary, appropriate professional advice is sought before making any decisions or taking any actions relating to the smart contract code analyzed in this report.

We would like to reiterate that the report is no replacement for a real, comprehensive audit involving significant manual labor. The report was performed mainly with automated tools.