ENIGMA DARK

Securing the Shadows

Security Review

Aave 3.4 Upgrade

Report produced for Aave DAO

Code developed by BGD Labs

May, 2025

Contents

1. Summary
2. Engagement Overview
3. Risk Classification
4. Vulnerability Summary
5. Findings
6. Disclaimer

Summary

Enigma Dark
Enigma Dark is a web3 security firm leveraging the best talent in the space to secure all kinds of blockchain protocols and decentralized apps. Our team comprises experts who have honed their skills at some of the best auditing companies in the industry. With a proven track record as highly skilled white-hats, they bring a wealth of experience and a deep understanding of the technology and the ecosystem.

Learn more about us at enigmadark.com

BGD Labs
BGD Labs is a Web3 development initiative and one of the main Aave contributors, responsible for the protocol's ongoing maintenance and the introduction of new, innovative features. Comprised of a team of expert developers with deep experience in Ethereum, more precisely in Decentralized Finance (DeFi), governance token modeling/economics.

AAVE 3.4 Protocol Upgrade
AAVE is one of the leading lending an borrowing platforms in DeFi, allowing users to supply and borrow assets with variable interest rates. The Aave 3.4 upgrade includes the following changes and features:

- Migration of the custom GHO on v3 Core to a standard a/v Token.
- Addition of Multi-call support on the Aave pool.
- Introduction of a new Position Manager role for a subset of user actions.
- Removal of the direct flash loan fee injection to suppliers opening to the DAO to re-distribute fees with suppliers and /or Umbrella stakers
- Many misscellaneous optimisations, striking a solid balance between UX/DevEx and infrastructure improvements.

Engagement Overview

Over the course of 2 weeks, beginning April 30 2025, the Enigma Dark team conducted a security review of the AAVE 3.4 Protocol Upgrade project. The review was performed by two Lead Security Researchers: vnmrtz & Lambda.

The following repositories were reviewed at the specified commits:

Repository	Commit
aave-dao/aave-v3-origin	`diff 464a0ea...bb66c4b`
bgd-labs/protocol-v3.4-upgrade	`e958112`, `d37769d`

Risk Classification

Severity	Description
Critical	Vulnerabilities that lead to a loss of a significant portion of funds of the system.
High	Exploitable, causing loss or manipulation of assets or data.
Medium	Risk of future exploits that may or may not impact the smart contract execution.
Low	Minor code errors that may or may not impact the smart contract execution.
Informational	Non-critical observations or suggestions for improving code quality, readability, or best practices.

Vulnerability Summary

Severity	Count	Fixed	Acknowledged
Critical	0	0	0
High	0	0	0
Medium	0	0	0
Low	0	0	0
Informational	1	1	0

Findings

Index	Issue Title	Status
I-01	Minor improvements to code and comments	Fixed

Detailed Findings

High Risk

No issues found.

Medium Risk

No issues found.

Low Risk

No issues found.

Informational

I-01 - Minor improvements to code and comments

Severity: Informational

Context: See below.

Technical Details / Recommendations:

1. FlashLoanLogic.sol#L202-L203 - `DataTypes.FlashLoanRepaymentParams` includes an unused parameter: `interestRateStrategyAddress`. Since the current flash loan logic no longer interacts with interest rates or modifies state, consider removing this parameter to simplify the struct.
2. FlashLoanLogic.sol#L188-L191, FlashLoanLogic.sol#L76-L79 - Comments reference an outdated part of the flash loan flow: updateState -> changeState -> updateRates. This flow has since been simplified and no longer interacts with state or interest rates. Recommend updating or removing these comments to reflect the current logic accurately.
3. LiquidationLogic.sol#L651-L653 - Variables are explicitly initialized to default values (0 and false), which is unnecessary in Solidity.
4. ReserveLogic.sol#L210-L211 - Comment incorrectly suggests that `_updateIndexes` modifies timestamps. However, this function only updates reserve indexes. Recommend correcting the comment.

Developer Response:

1. The removal of ir update was actually a bug.
2. Due to 1) we reintroduced it in commit `c0bd6b9`.

3. Its unnecessary but there is no gas impact and we consider it more readable / clearer to be explicit.
4. Addressed in commit `bb66c4b`.

Fixed. The fixes have been verified by the Enigma Dark team.

Disclaimer

This report does not endorse or critique any specific project or team. It does not assess the economic value or viability of any product or asset developed by parties engaging Enigma Dark for security assessments. We do not provide warranties regarding the bug-free nature of analyzed technology or make judgments on its business model, proprietors, or legal compliance.

This report is not intended for investment decisions or project participation guidance. Enigma Dark aims to improve code quality and mitigate risks associated with blockchain technology and cryptographic tokens through rigorous assessments.

Blockchain technology and cryptographic assets inherently involve significant risks. Each entity is responsible for conducting their own due diligence and maintaining security measures. Our assessments aim to reduce vulnerabilities but do not guarantee the security or functionality of the technologies analyzed.

This security engagement does not guarantee against a hack. It is a review of the codebase during a specific period of time. Enigma Dark makes no warranties regarding the security of the code and does not warrant that the code is free from defects. By deploying or using the code, the project and users of the contracts agree to use the code at their own risk. Any modifications to the code will require a new security review.