Security Assessment & Formal Verification Report

Stable Rate Removal

Oct-2024

Prepared for

BGD Labs on Aave

Table of content

certora BORED GHOSTS DEVELOPING aave

Project Summary

Project Scope

Project Name	Repository (link)	Latest Commit Hash	Platform
stable-removal	https://github.com/aave-dao/aave-v3-origin	be45428	EVM/Solidity 0.8

Project Overview

This document describes the specification and verification of the **stable rate removal** using the Certora Prover and manual code review findings. The work was undertaken from **25 Aug2024 to 10 Sep 2024**.

The following contract list is included in our scope:

- Aave's Pool

The Certora Prover demonstrated that the implementation of the Solidity contracts above is correct with respect to the formal rules written by the Certora team. In addition, the team performed a manual audit of all the Solidity contracts**.** During the verification process and the manual audit, no bug was discovered. (Anyhow we have one informational issue that we list below.)

Project Overview

In Aave-v3.2.0 several changes were introduced. One of them is the removal of all the solidity code that is relevant to stable debt allowances.

Coverage

The Stable Debt deprecation process involves a thorough overhaul of various core components within the Aave system, focusing on eliminating references to stable debt tokens while ensuring backward compatibility in certain areas.

1. We wrote a new rule in order to check the deprecation of the stable rate mechanism. See more information later.
2. We ran the already existing rules of the Pool.
3. With respect to manual auditing we have checked the following:
    - We have checked that references in the code of stable/stoken/debt/token which are related to stable debt have been removed or have been kept for backward compatibility.

Findings Summary

The table below summarizes the findings of the review, including type and severity details.

Severity	Discovered	Confirmed	Fixed
Critical			
High			
Medium			
Low			
Informational	1		
Total			

Severity Matrix

Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		Likelihood		

Detailed Findings

ID	Title	Severity	Status
I-01	Events still keep the stable debt token reference.	Informational	

Informational Severity Issues

I-01. Events still keep the stable debt token reference.

Description: In the PoolConfigurator the following events still refer to the stable debt token:

event ReserveInitialized still contains stableDebtToken
event ReserveStableRateBorrowing
event StableDebtTokenUpgraded

Recommendation: Remove these events.
BGD Labs response: `ReserveStableRateBorrowing` and `StableDebtTokenUpgraded` have been removed. `ReserveInitialized` is emitted with `stableDebtToken` being constant `address(0)` for backwards compatibility on systems indexing the events.

Formal Verification

Verification Notations

Formally Verified	The rule is verified for every state of the contract(s), under the assumptions of the scope/requirements in the rule.
Formally Verified After Fix	The rule was violated due to an issue in the code and was successfully verified after fixing the issue
Violated	A counter-example exists that violates one of the assertions of the rule.

Formal Verification Properties

In the table below we specify all the formally verified rules that we wrote for the verification of the stable rate removal, and give a detailed description for them. A link to the Certora's prover report can be found here.

P-01. No Writes Access to the Deprecated Stable Fields

Status: Verified	Property Assumptions:

Rule Name	Status	Description	Rule Assumptions
stableFieldsUntouched	Verified	*Check that the values in the following deprecated fields are not changed, and are not accessed for writing: __deprecatedStableBorrowRate,__deprecatedStableDebtTokenAddress. (These are fields of the struct DataTypes.ReserveData)*	*None*

Disclaimer

The Certora Prover takes a contract and a specification as input and formally proves that the contract satisfies the specification in all scenarios. Notably, the guarantees of the Certora Prover are scoped to the provided specification and the Certora Prover does not check any cases not covered by the specification.

Even though we hope this information is helpful, we provide no warranty of any kind, explicit or implied. The contents of this report should not be construed as a complete guarantee that the contract is secure in all dimensions. In no event shall Certora or any of its employees be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with the results reported here.

About Certora

Certora is a Web3 security company that provides industry-leading formal verification tools and smart contract audits. Certora's flagship security product, Certora Prover, is a unique SaaS product that automatically locates even the most rare & hard-to-find bugs on your smart contracts or mathematically proves their absence. The Certora Prover plugs into your standard deployment pipeline. It is helpful for smart contract developers and security researchers during auditing and bug bounties.

Certora also provides services such as auditing, formal verification projects, and incident response.