Security Assessment & Formal Verification Report

Upgradeable GHO

May-2024

Prepared for
AAVE

Table of content

Project Summary

Project Scope

Project Name	Repository (link)	Latest Commit Hash	Platform
Upgradable GHO	aave-gho-core	a9647e1	EVM/Solidity 0.8

Project Overview

This document describes the specification and verification of the **Upgradable GHO** using the Certora Prover and manual code review findings. The work was undertaken from **8 May 2024** to **11 June 2024**.

The scope of our review is the following contracts:

- UpgradeableGhoToken
- UpgradeableERC20

We note that we only checked upgradability aspects of these contracts.

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.)

Protocol Overview

The contract under review is a modified version of the GhoToken contract, incorporating a feature that enables upgrades to the contract logic. This enhancement allows for logic upgrades, facilitating future adaptations as required. The modifications consist of minor adjustments to the deployment sequence of the token base contract and the incorporation of the transparent proxy pattern.

For a detailed list of modifications, please refer to the PR in the repository.

Coverage

1. We ran the already existing rules of the GHO token, on the UpgradeableGhoToken and made sure they all pass.
2. We performed a manual auditing while focusing on the upgradability of the contract.

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	Using a deprecated function	Informational	Fixed

Informational Severity Issues

I-01. Using a deprecated function

Description: In the contract UpgradeableGhoToken there is a call to _setupRole() which is deprecated. According to OpenZeppelin docs setupRole() is deprecated in favor of _grantRole().

Recommendation: Consider calling _grantRole() directly instead.

Aave Labs response: Fixed.

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.