

# **Security Assessment Report**



# Permissioned Payloads Controller

April-2025

Prepared for:

**Aave DAO** 

Code developed by:







## Table of content

Project Summary	3
Project Scope	
Project Overview	
Protocol Overview	
Findings Summary	4
Severity Matrix	4
Detailed Findings	5
Audit Goals	5
Coverage and Conclusions	5
Disclaimer	6
About Certora	6





# **Project Summary**

#### **Project Scope**

Project Name	Repository (link)	Latest Commit Hash	Platform
Aave Permissioned Payloads Controller	Github Repository	0183572	EVM

### **Project Overview**

This document describes the verification of **Aave Permissioned Payloads Controller** code using manual code review. The work was undertaken from **April 28** to **April 30**, **2025**.

The following contracts are considered in scope for this review:

- src/contracts/payloads/PayloadsControllerCore.sol
- src/contracts/payloads/PermissionedPayloadsController.sol
- src/contracts/payloads/WithPayloadsManager.sol
- src/contracts/payloads/interfaces/IWithPayloadsManager.sol
- src/contracts/payloads/interfaces/IPermissionedPayloadsController.sol
- src/contracts/libraries/Errors.sol

The team performed a manual audit of all the solidity contracts. During the audit, Certora didn't find any significant issues in the code.

#### **Protocol Overview**

The **Permissioned Payloads Controller** is an extension of the existing PayloadsController contract. It grants a set of privileges to a Guardian and a PayloadsManager to manage low risk parameters of Aave in a similar manner than governance. This design allows any changes to be reviewed, validated and cancelled if necessary. The implementation also maintains access control over the parts of Aave the payloads are able to change thanks to a newly deployed Executor contract with restricted permissions, providing safeguard regarding the protocol configuration.



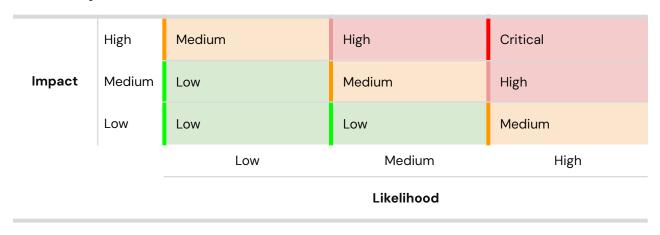


## **Findings Summary**

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

Severity	Discovered	Confirmed	Fixed
Critical	-	-	-
High	-	-	-
Medium	-	-	-
Low	-	-	-
Informational	-	-	-
Total	_	_	_

## **Severity Matrix**







# **Detailed Findings**

#### **Audit Goals**

- 1. Since the payload controller allows a permissioned (possibly centralized) entity to submit unrestricted data without going through standard governance procedure, safeguards should apply on the executor to prevent control over the entire system.
- 2. Payload cancellation should only be triggered by the guardian and the payloadsManager.
- 3. Payload creation should only be triggered by the payloadsManager.
- 4. Possible timelock (delay) value should be bounded.
- 5. Timelock (delay) should only be configured by the guardian.

### **Coverage and Conclusions**

- 1. The contract is deployed alongside a dedicated Executor separate from the existing ones. The new Executor will be granted special roles, authorizing it to perform a specific set of actions with respect to the Aave ecosystem, e.g. manage umbrella rewards. This ensures that actions submitted through PermissionedPayloadController cannot alter critical protocol parameters outside the authorized scope.
- 2. The function responsible for payload cancellation overrides the default implementation and adds a onlyPayloadsManagerOrGuardian modifier to provide access control.
- 3. The function responsible for payload creation overrides the default implementation and adds a onlyPayloadsManager modifier to provide access control, allowing only this trusted address to create and queue payloads.
- 4. The timelock can only be set to a value between 0 days and 7 days, both included.
- 5. The function responsible for modifying the timelock is restricted with the onlyGuardian modifier.





# Disclaimer

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.