Aergo (HPP) - Vesting

Security Assessment

CertiK Assessed on Dec 2nd, 2025

CertiK Assessed on Dec 2nd, 2025

Aergo (HPP) - Vesting

The security assessment was prepared by CertiK.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Staking	EVM Compatible	Formal Verification, Manual Review, Static Analysis

LANGUAGE	TIMELINE
Solidity	Preliminary comments published on 12/02/2025
	Final report published on 12/04/2025

Vulnerability Summary

2	0	0	2	0
Total Findings	Resolved	Partially Resolved	Acknowledged	Declined

1	Centralization	1 Acknowledged	Centralization findings highlight privileged roles & functions and their capabilities, or instances where the project takes custody of users' assets.
0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
0	Major		Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.
0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
0	Minor		Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
1	Informational	1 Acknowledged	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | AERGO (HPP) - VESTING

CODEBASE | AERGO (HPP) - VESTING

Repository

https://github.com/hpp-io/contracts/blob/main/contracts/HPP_Vesting_AIP21.sol

Commit

123f5838bcee7c6c13734b4ec30ff5ec2155af2b

AUDIT SCOPE | AERGO (HPP) - VESTING

hpp-io/contracts

HPP_Vesting_AIP21.sol

APPROACH & METHODS | AERGO (HPP) - VESTING

This audit was conducted for Aergo (HPP) to evaluate the security and correctness of the smart contracts associated with the Aergo (HPP) - Vesting project. The assessment included a comprehensive review of the in-scope smart contracts. The audit was performed using a combination of Formal Verification, Manual Review, and Static Analysis.

The review process emphasized the following areas:

- Architecture review and threat modeling to understand systemic risks and identify design-level flaws.
- Identification of vulnerabilities through both common and edge-case attack vectors.
- Manual verification of contract logic to ensure alignment with intended design and business requirements.
- Dynamic testing to validate runtime behavior and assess execution risks.
- Assessment of code quality and maintainability, including adherence to current best practices and industry standards.

The audit resulted in findings categorized across multiple severity levels, from informational to critical. To enhance the project's security and long-term robustness, we recommend addressing the identified issues and considering the following general improvements:

- Improve code readability and maintainability by adopting a clean architectural pattern and modular design.
- Strengthen testing coverage, including unit and integration tests for key functionalities and edge cases.
- Maintain meaningful inline comments and documentations.
- Implement clear and transparent documentation for privileged roles and sensitive protocol operations.
- Regularly review and simulate contract behavior against newly emerging attack vectors.

REVIEW NOTES | AERGO (HPP) - VESTING

Overview

The `HPP_Vesting_AIP21` contract implements a linear vesting program. It manages the distribution of HPP tokens to multiple beneficiaries over a fixed 24-month duration.

Key features include:

- **Global Vesting Clock**: Vesting follows a single global `vestingStartTime` for all beneficiaries.
- **Linear Distribution**: Tokens vest linearly over a 730-day period (approx. 24 months) starting from the global start time.
- **Owner-Managed Registry**: The owner is responsible for initializing the start time and adding beneficiaries (individually or in batches).
- **Retroactive Allocation**: Schedules can only be added *after* the vesting start time is set, meaning new beneficiaries immediately have a portion of tokens vested based on the time elapsed since the start.
- **Revocability**: The owner can revoke a beneficiary's schedule, effectively cancelling their right to claim any further tokens (including those already vested but unclaimed).
- **Emergency Controls**: The contract includes mechanisms for the owner to withdraw funds.

External Dependencies

- **OpenZeppelin**: `IERC20`, `SafeERC20`, `EnumerableSet`, `Ownable`, `ReentrancyGuard`.
- The contract integrates with a specific ERC20 token (`hppToken`) set at deployment. The token is expected to follow standard ERC20 behavior.

Privileged Functions

Functions callable only by the owner that significantly impact contract state and funds:

- `startVesting`: Permanently sets the global `vestingStartTime` and enables the addition of schedules.
- `addVestingSchedule`, `addVestingSchedules`: Assigns token allocations to beneficiaries. Requires vesting to be started.
- `revokeVestingSchedule`: Deactivates a beneficiary's schedule. This prevents any future claims, including tokens that calculated as vested based on time but were not yet claimed.
- `emergencyWithdraw`, `emergencyWithdrawAll`: Allows the owner to sweep tokens from the contract to the owner address. This capability effectively allows the owner to override token reservations for vesting schedules.

Because the owner has absolute control over creating schedules, revoking claims, and draining contract funds, the owner account represents a single point of failure and should be secured via a multisig or timelock.

FINDINGS | AERGO (HPP) - VESTING

2	0	1	0	0	0	1
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational

This report has been prepared for Aergo (HPP) to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 2 issues were identified. Leveraging a combination of Formal Verification, Manual Review & Static Analysis the following findings were uncovered:

ID	Title	Category	Severity	Status
AHV-01	**Centralization Risks In Source**	**Centralization**	**Centralization**	**Acknowledged**
AHV-02	Backdated Vesting Start Lets Late Beneficiaries Claim Allocation Immediately	Design Issue	Informational	Acknowledged

AHV-01 | Centralization Risks In Source

Category	Severity	Location	Status
Centralization	**Centralization**	**source: 84, 100, 128, 213, 232, 243**	**Acknowledged**

Description

In the contract `HPP_Vesting_AIP21` the role `_owner` has authority over the functions shown in the diagram below (`startVesting`, `addVestingSchedule`, `addVestingSchedules`, `revokeVestingSchedule`, `emergencyWithdraw` and `emergencyWithdrawAll`). Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and add for anyone vestingSchedules or withdraw all the tokens held by this contract.

Recommendation

It's recommended that the project reduces reliance on single privileged accounts by implementing decentralized mechanisms for sensitive contract operations. In the short term, introduce a timelock for all critical functions and transfer privileged roles to a multisignature wallet to prevent unilateral control and enable greater operational transparency. Publicly document these changes, including timelock contracts and multisignature addresses. For a more robust, long-term solution, integrate a governance module or DAO to shift operational authority to the community while maintaining timelocks for transparency and security. Ultimately, fully decentralize the contract by either renouncing ownership or removing high-risk privileged functions that no longer require central oversight.

Alleviation

[Aergo (HPP), 12/03/2025]: The team acknowledged the issue and decided not to implement the recommended change in the current engagement.

AHV-02 Backdated Vesting Start Lets Late Beneficiaries Claim Allocation Immediately

Category	Severity	Location	Status
Design Issue	Informational	HPP_Vesting_AIP21.sol: 109~116	Acknowledged

Description

`_addVestingSchedule` stamps every new schedule with the original `vestingStartTime`. Because adding schedules is only permitted after `vestingStarted` is true, any beneficiary onboarded after TGE inherits the past start time, and `_getVestedAmount` treats the entire elapsed period as vested, allowing near-instant withdrawal.

```
    function _addVestingSchedule(address _beneficiary, uint256 _amount) private {
        require(_beneficiary != address(0), "Invalid beneficiary address");
        require(_amount > 0, "Amount must be greater than 0");
        require(!vestingSchedules[_beneficiary].isActive, "Vesting schedule already
exists");
        require(vestingStarted && vestingStartTime != 0, "Vesting not started");
        vestingSchedules[_beneficiary] = VestingSchedule({
            beneficiary: _beneficiary,
            totalAmount: _amount,
            claimedAmount: 0,
            startTime: vestingStartTime,
            duration: VESTING_DURATION,
            isActive: true
        });
        beneficiaries.add(_beneficiary);
        totalVestingAmount += _amount;
        emit VestingScheduleAdded(_beneficiary, _amount, vestingStartTime);
    }
```

Recommendation

(If this is not a intended design)Decouple individual schedule start times from the global start. Either (a) allow schedules to be created before `startVesting` so all beneficiaries share the same true start, or (b) set each schedule's `startTime` when it is created (e.g., `block.timestamp`) and optionally adjust duration or cliff to reflect program rules. Additionally, enforce per-beneficiary cliffs if uniform start alignment is required.

Alleviation

[Aergo (HPP), 12/03/2025]: The team acknowledged the issue and confirmed this is an intended design.

APPENDIX | AERGO (HPP) - VESTING

Finding Categories

Categories	Description
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Elevating Your Web3 Journey

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is the largest blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.