Audited by Pashov Audit Group.

A time-boxed security review of every AURORA contract, 7 to 10 September 2026, by eight researchers from Pashov Audit Group. Every finding was answered, fixed where a fix was warranted, and re-reviewed by the auditors before this report was issued. The full report is below, unedited.

Read the report below

See the accountants live

01 Summary

CRITICAL
0
none found

HIGH
0
none found

MEDIUM
6
6 fixed

LOW
11
11 fixed

INFORMATIONAL
24
18 fixed · 6 acknowledged

41 findings in total. Every medium and low severity finding was fixed and the fix was reviewed by Pashov. Six informational findings were acknowledged with a written reason, reproduced in the report and summarised in section 04 below. No finding was disputed.

02 Scope

Auditor

Pashov Audit Group

Review window

7 - 10 September 2026

In scope

every contract under src/: StripVault, MultiplierAccountant, AuroraMorphoOracle, principal and yield tokens, deployment factory

Reviewed commit

2e780ae78beba72b8342ee9ef590ce420cb4356f

Fixes reviewed at

3dfa4a421d5d9d1fc2849f1847619e3b7dbf2ddb

Researchers

0x37, 0xApple, 0xbrivan, Auditor-Nate, farismaulana, LoopGhost, Playboi, Valves Security

The review repository is a private mirror shared with the auditors, so the commit links inside the PDF are not public. The source of every deployed contract is verified on Address hidden, and the audited build is identified by the commit hash above.

03 What happens next

NOW

The contracts live on mainnet today are the reviewed build. Four series have run on them since launch. Merge is permissionless and always open on every vault, before and after maturity.

NEXT

The fixed build goes live. New vaults, accountants and oracle at the fixes commit, verified on chain. Addresses are swapped in on every page of this site and published on the oracle page, and existing positions can merge out of the old vaults at any time.

THEN

Lending opens and the series cap comes off. The Morpho market is treasury-only until the fixed oracle is deployed. Deeper pools and new series follow.

04 Acknowledged findings

Six informational findings were acknowledged rather than changed. The auditors' reasoning and ours are in the report; the short version of each is here.

I-04 · I-06 · I-12 — feed freshness during trading hours

The Morpho oracle accepts a Chainlink stock price up to four days old so that weekends and market holidays do not freeze the market. That single window is wider than the feed's heartbeat during trading hours, so a feed that halts mid-session would not be caught by the age check alone. There is no second stock price feed or market-status feed on Robinhood Chain to corroborate against today. **Mitigated by the 62.5% LLTV buffer and documented as an operational risk.** A liveness check is planned for a follow-up review once a corroborating feed exists on the chain.

`I-09 — split ratio tolerance`

A residual inside the split tolerance (one millionth of the ratio) is attributed to the split, not to yield. The smallest real dividend on a covered stock is about a thousand times larger than the tolerance, so a genuine split combined with a real dividend cannot pass the clean-ratio check and goes to guardian decomposition instead. **Kept as designed and documented.**

`I-15 · I-20 — rounding at the eighteenth decimal`

Both redemption legs round down independently, which can strand one raw unit (10^{-18} of a stock token) per matched redemption, and each dividend classification floors once, drifting the index by a few units at the same scale over a series' life. Both round in the vault's favour so it can never owe more than it holds. **Kept; the alternatives add arithmetic to the core index for an attowei-level gain.**

05 All 41 findings

ID	Finding	Severity	Status
M-01	Two `unsynced` multiplier applies are recorded as one non-collapsed composite stamped at the LAST action's `effectiveAt`, same YT wipe, a distinct root cause	MEDIUM	FIXED
M-02	USD-denominated feed is used as loan-token value without a loan-token/USD conversion	MEDIUM	FIXED
M-03	Guardian resolution commitment can be reused after pending endpoints cycle	MEDIUM	FIXED
M-04	Collapsed multiplier changes reuse the first update timestamp for all decomposed actions	MEDIUM	FIXED
M-05	Manipulable Uniswap V3 TWAP can force premature PT liquidations	MEDIUM	FIXED
M-06	Settled PT oracle lacks a redemption-value floor	MEDIUM	FIXED
L-01	Holiday holds cross the immutable 4-day staleness gate because the feed stops printing hours before every close, freezing every Morpho market this oracle prices through the reopen	LOW	FIXED

ID	Finding	Severity	Status
L-02	Magnitude-only dividend classification force-tags value-neutral in-band multiplier changes, permanently shifting PT principal to YT holders	LOW	FIXED
L-03	Oracle accepts a feed during the L2 sequencer recovery window	LOW	FIXED
L-04	Oracle resumes PT valuation before the post-dividend TWAP reflects the PT repricing	LOW	FIXED
L-05	Oracle scaling is incorrect when stock and PT base-unit decimals differ	LOW	FIXED
L-06	Pending guardian resolution becomes stale when sync collapses a later multiplier update	LOW	FIXED
L-07	Pending multiplier endpoint equality hides intermediate updates	LOW	FIXED
L-08	Per-call fee truncation permits fee-free micro-splits and YT redemptions	LOW	FIXED
L-09	Per-call split-fee rounding permits fee-free fragmented deposits	LOW	FIXED
L-10	Per-call YT fee rounding allows yield-fee avoidance through fragmented redemptions	LOW	FIXED
L-11	YT redemption fee can be bypassed through fragmented redemptions	LOW	FIXED
I-01	Multiplier processing can become unavailable because deployment accepts a zero administrator	INFO	FIXED
I-02	Fees remain trapped and the deposit cap can be exceeded because the vault accepts itself as treasury	INFO	FIXED
I-03	Guardian recovery can be delayed because malformed proposals overwrite valid resolutions	INFO	FIXED
I-04	Timestamp freshness accepts economically stale feed answers	INFO	ACKNOWLEDGED

ID	Finding	Severity	Status
I-05	Immutable feed-decimal snapshot becomes stale after same-address feed migration	INFO	FIXED
I-06	Chainlink feed can remain stale while the onchain stock market remains active	INFO	ACKNOWLEDGED
I-07	Accountant sync can clear while the Robinhood price feed remains deliberately paused	INFO	FIXED
I-08	The oracle can bypass the PT vault's synchronization gate because its accountant is independently configured	INFO	FIXED
I-09	Split tolerance can absorb a real dividend without crediting YT	INFO	ACKNOWLEDGED
I-10	Shape-only split classification routes value-additive clean-ratio events entirely into splitFactor, zeroing the YT drip at settlement	INFO	FIXED
I-11	Immediate Multiplier Updates Can Be Missed at the Maturity Boundary	INFO	FIXED
I-12	Four-Day Feed Freshness Window Accepts Stale Prices During Active Trading	INFO	ACKNOWLEDGED
I-13	accruedDripFactor exposes unsynchronized live index instead of a settlement-compatible value	INFO	FIXED
I-14	Disabled feed-age validation accepts unfinished Chainlink rounds	INFO	FIXED
I-15	Independent PT and YT redemption rounding strands matched-position dust	INFO	ACKNOWLEDGED
I-16	No recovery path for residual stock after all PT and YT liabilities are extinguished	INFO	FIXED
I-17	Oracle Constructor Does Not Validate That the Pool Contains the Accountant's Stock Token	INFO	FIXED
I-18	Oracle does not unconditionally reject incomplete Chainlink rounds	INFO	FIXED
I-19	Post-maturity accountant changes can block settlement of an otherwise mature vault	INFO	FIXED

ID	Finding	Severity	Status
I-20	Repeated dividend classification introduces cumulative downward index rounding drift	INFO	ACKNOWLEDGED
I-21	Split classification stores the rounded observed ratio instead of the validated clean ratio	INFO	FIXED
I-22	Unsettled accruedDripFactor includes dividends occurring after maturity	INFO	FIXED
I-23	Untracked token donations can permanently exhaust StripVault deposit capacity	INFO	FIXED
I-24	Zero guardian delay removes the configured resolution reaction window	INFO	FIXED

Titles as written by the auditors. Each finding in the PDF carries a summary, impact, exploit path where applicable, the recommendation and our resolution.

AURORA · reviewed by Pashov Audit Group · Robinhood Chain 4663 report PDF · docs