AREXAI

Internal Security Review

Automated analysis, reviewed notices and operational risk boundaries

NETWORK	REVIEW DATE	STATUS
BNB Smart Chain - 56	14 September 2026 UTC	INTERNAL REVIEW

Important scope notice

This document provides technical transparency. It is an internal engineering review, not an independent security audit, a guarantee of safety, legal approval or investment assurance.

Release baseline: b61217f
Solidity: 0.8.24 with optimizer, 200 runs
Token: 0xeaa12b3be7cdec7749b972ed5c342f4e933ccbb3

1. Conclusion

No critical or high-severity finding was reported by the local automated checks. Nine Hardhat tests passed. Slither ran 102 detectors over the production contracts and reported six notices: five timestamp-dependence notices and one exact-zero comparison. Manual review classified these as intentional schedule and release controls, not demonstrated exploits.

2. Evidence

Check	Result
Hardhat tests	9 passed, 0 failed
Statement coverage	96.43%
Function coverage	90.00%
Line coverage	95.24%
Branch coverage	47.12%
Slither	102 detectors; 0 critical/high findings; 6 reviewed notices
Published source	Six contracts; Sourcify exact creation/runtime matches

3. Reviewed Slither notices

- Timestamp dependence in presale start, end and finalization checks is required to enforce immutable sale windows.
- Timestamp dependence in team vesting and LP-token release is required to enforce configured unlock schedules.
- The exact-zero comparison in LPTokenLocker.release() intentionally rejects an empty release after unlock.

These classifications describe intended behavior; they do not eliminate validator timestamp tolerance or unknown risks.

4. Material operational risks

01

The same externally owned cold-wallet address is admin, treasury and allocation beneficiary. Loss, compromise or incorrect signing affects several controls at once.

02

The 100M marketing allocation has no on-chain vesting lock and is held by the admin wallet.

03

Listing and liquidity reserves are owner-controlled release vaults and require operational governance and public disclosure.

04

The liquidity vault holds ARXAI, not PancakeSwap LP tokens. A separate LPTokenLocker must be deployed and funded after the real pool exists.

05

Presale purchases are irreversible. Buyers must use the supported BSC purchase flow and retain BNB for network fees.

06

Branch coverage of 47.12% indicates that additional negative-path and boundary tests would improve assurance.

07

International availability creates legal, sanctions, consumer-protection, tax and KYC/AML questions that code does not solve.

5. Required release gates

- Complete an independent third-party audit before broad public fundraising.
- Obtain jurisdiction-specific legal and compliance review.
- After Round 1 opens, execute one 100 USDT purchase from a separate buyer wallet and reconcile buyer ARXAI, treasury USDT and the TokensPurchased event.
- Publish verified contract addresses and explicit network/payment-token warnings.
- Define incident-response signers and migrate contract ownership to a tested multisignature wallet when ready.
- After liquidity creation, deploy the LP-token locker with at least a six-month unlock, transfer the actual LP tokens and publish the transactions.