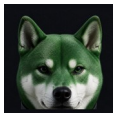

Internal Security Audit

PSUSD Final Security Audit Report

BSC and Base contract review, live-state verification, and post-hardening assessment

Date: 2026-07-04

Audit execution: Internal AI-assisted security review executed by GitHub Copilot using GPT-5.4, based on repository source inspection, live chain-state verification, operational hardening evidence, and backend validation performed on the current PSUSD deployment.

Scope: BSC and Base PSUSD contracts. **Live result:** hardened in place. **Residual risk:** moderate.

Outcome: The PSUSD live deployment was hardened in place without redeploying the core contracts. Security posture improved materially, but the final target state has not yet been fully reached.

Before: high operational centralization risk. **After:** moderate residual operational risk.

Executive Summary

This report covers the PSUSD BSC and Base contract stack, the live production deployment state, and the security hardening actions completed during this audit cycle.

- The PSUSD Solidity contracts were reviewed at source level, including the strict bridge token path, mirrored reserve logic, Base redemption vault, async redeem coordinator, rebalancer support contracts, and supporting router surface.
- The live deployment on BSC and Base was verified directly at address level for ownership, fee-recipient posture, reserve and rebalancer roles, and final paused / unpaused state.
- Security posture improved materially through in-place hardening without redeploying the core PSUSD contracts.
- The main remaining residual risks are owner multisig migration, reserve / rebalancer key separation, and explicit bytecode / source parity confirmation for the live Base async redeem coordinator.
- This document should be presented as an internal AI-assisted security audit and hardening cycle, not as a third-party certification.

Scope

- `PSUSDCanonicalBridgeMintBurnAttested.sol`
- `PSUSDCanonicalBridgeMintBurnAttestedRedeemable.sol`
- `PSUSDCanonicalBridgeMintBurnAttestedMirroredReserve.sol`
- `PSUSDCanonicalBridgeMintBurnAttestedMirroredReserveStrict.sol`
- `PSUSDSatelliteRedemptionVault.sol`
- `PSUSDBaseAsyncRedeemCoordinator.sol`
- `PSUSDReserveRebalancerCoordinator.sol`
- `PSUSDAutoMintRouter.sol`
- Live backend relayer and async redeem services on Hetzner VPS

Live Deployment Covered

- BSC strict token: `0x71Dab0d2954Cf9Ae7F9Ccb5E4AD4044497c4B24E`
- Base strict token: `0x17ce373E51d652941Ee3B4c81fA04800Ba12E151`
- Base vault: `0xE6666A6Ed1fD2E7B73038aC6B4BFce20f3E4521b`
- Base async redeem coordinator documented live: `0x9353D661064A71bAa360238D4bBE7A2446C36DE9`

Contract-by-Contract Coverage

PSUSDCanonicalBridgeMintBurnAttested.sol

Network / role: core strict bridge token logic for the live BSC and Base strict token family

Coverage: Source reviewed and live ownership / role state checked.

Main notes: Source review identified surplus-attribution risk in the strict attested path.

Repository hardening exists; live conclusions remain tied only to explicitly verified

deployment state.

PSUSDCanonicalBridgeMintBurnAttestedRedeemable.sol

Network / role: redeemable strict-token extension

Coverage: Source reviewed.

Main notes: No separate standalone critical issue was isolated in this pass beyond inherited owner / operator concentration risk.

PSUSDCanonicalBridgeMintBurnAttestedMirroredReserve.sol

Network / role: reserve mirroring and reserve-release logic

Coverage: Source reviewed.

Main notes: Repository review identified the need to bind reserve release to real bridge demand and approved recipients.

PSUSDCanonicalBridgeMintBurnAttestedMirroredReserveStrict.sol

Network / role: strict mirrored reserve configuration on the live strict deployment family

Coverage: Source reviewed and live role state verified.

Main notes: Operationally important because it sits on the live BSC/Base strict token path.

Residual live risk is mainly role concentration.

PSUSDSatelliteRedemptionVault.sol

Network / role: live Base vault

Coverage: Source reviewed and live ownership / fee recipient / rebalancer state verified.

Main notes: Owner and fee-recipient posture improved. Rebalancer concentration remains an open residual risk.

PSUSDBaseAsyncRedeemCoordinator.sol

Network / role: documented live Base async redeem coordinator

Coverage: Source reviewed and live deployment status partially checked.

Main notes: Repository source includes stronger pause / cancel behavior. Live bytecode / source parity remains a follow-up item.

PSUSDReserveRebalancerCoordinator.sol

Network / role: off-chain-assisted reserve rebalancer support contract

Coverage: Source reviewed.

Main notes: Repository hardening added duplicate active-request blocking. Residual live concern is operational key concentration.

PSUSDAutoMintRouter.sol

Network / role: supporting mint / route coordination component

Coverage: Source reviewed.

Main notes: Included in code-review scope. No standalone live critical issue was elevated above the broader PSUSD admin and operator control risks in this pass.

Completed Live Hardening

- Owner rotated to `0xc6dB5C0d67A2e6F8556acE7f3e0d8cDD916286Da`
- Fee recipient rotated to `0x293Be3DB5cdD11c2CeA7D739626ba910322926F9`
- Relayer rotated to `0xCDb08A6ee057AbFeA7BD4b2F4A3c3A536cae5A8D`
- Reserve operator intentionally unchanged: `0x756f2Ee96B7c57932FDFf8090cb671C177958110`
- Base rebalancer intentionally unchanged: `0x756f2Ee96B7c57932FDFf8090cb671C177958110`

Methodology

1. Manual source review of bridge, reserve, redeem, coordinator, and privilege surfaces.
2. Repository build and regression validation.
3. Live chain state verification on BSC and Base.
4. In-place role hardening on the live deployment.
5. VPS relayer rotation and service verification.
6. Async redeem doctor, dry-run checks, and shadow smoke testing.

Findings

Medium - Contract-level issues were identified in the PSUSD Solidity codebase and addressed in repository hardening work

The contract review portion of this audit covered the PSUSD Solidity code itself, not only the live operational setup. That review identified important code-level areas around surplus attribution, reserve release controls, and operator-assisted guardrails in async / rebalancer support contracts.

Impact: these were real contract-level security and correctness concerns in the reviewed codebase, especially for future deployments or parity-sensitive live components.

Recommendation: keep the hardened repository implementations as the source of truth for future deployments and verify live bytecode parity where operationally relevant.

Medium - Owner role is improved but still EOA-based

The live owner is no longer the original concentrated operational wallet, but it is still a single EOA rather than a multisig.

Impact: compromise of the new owner EOA would still allow owner-level reconfiguration.

Recommendation: migrate owner to a multisig.

Medium - Reserve operator and Base rebalancer remain concentrated

The reserve-moving role and the Base vault rebalancer are still on the legacy hot wallet.

Impact: reserve and liquidity operations still have a larger-than-ideal blast radius.

Recommendation: split these hot roles when operations are ready.

Medium - Live async redeem coordinator may lag hardened local source

The local repository contains stronger async control logic than what was earlier observed on the documented live coordinator deployment.

Impact: emergency assumptions for the async redeem coordinator should be treated cautiously until bytecode parity is confirmed.

Recommendation: perform explicit live bytecode/source parity verification for the coordinator.

Informational - Core PSUSD contracts were not redeployed

This hardening cycle intentionally preserved live contract addresses and existing integrations.

Repository Hardening vs Live State

The repository source tree contains additional hardening work beyond the live in-place role rotation.

- Surplus accounting hardening for collateral attribution.
- Reserve release hardening bound to approved recipients and pending reserve budget.
- Async redeem pause and user cancellation behavior.
- Rebalancer duplicate active-request blocking.

Important distinction: this audit explicitly separates contract-level source hardening from what was directly verified on live deployed contracts. The PSUSD BSC and Base contracts were part of the audit scope, but live conclusions are intentionally limited to state and behavior that were directly validated.

Validation Summary

- Owner transfer BSC strict token: `0x765edb258bdb2e9deb39e7f5be70e31d03dbb2519f7879e730d2e1378392a15a`
- Owner transfer Base strict token: `0xccaa93cb31af2ed85759eca3cc547fae053a5b9b5306a31f44ebda028fa01132`
- Owner transfer Base vault: `0x0edf14bb071e2020190d2e83eea7a2b613fe1fb0c713de975a02d68a996724f5`
- Unpause BSC strict token: `0xa29936b049aafb6a78c58b206c243809cb51bde070b7e6519b850a0ac70b4157`
- Unpause Base strict token: `0x4795e846ca38a61daec5ae455a100ad886326a6a63e07bb2f350b2f53769cfe7`
- Unpause Base vault: `0x3bbc339441be3a6023e7db68da005ccec15dc04d6478cb2c291308e0c5f747ac`
- Backend health: OK
- Async redeem doctor: OK
- Async redeem worker dry-run: OK
- Async redeem claim worker dry-run: OK
- Async redeem shadow smoke test: OK

Conclusion

This audit cycle produced a real live security improvement. The deployment is safer than before, but not yet at its ideal end state.

Priority next steps are: multisig owner migration, reserve operator / rebalancer split, and explicit live coordinator parity verification.