MIDWEST SMART CONTRACTS
SMART-CONTRACT SECURITY REVIEW

BAD MINNIE

Claim Distributor v1.1

Source-Level Re-audit Report

RESULT M-01 is remediated in the reviewed v1.1 source. No Critical, High, or Medium-severity vulnerabilities remain open. Source-level re-audit accepted; production build and Mainnet deployment verification remain pending.

Report ID	Version	Review date	Status
MSC-MINNIE-READUD-2026-002	1.1	6 September 2026	Accepted / deployment gates pending

Reviewed artifact

Artifact	SHA-256
MINNIE-Claim-Distributor-v1.1-Reaudit(1).zip	dd1ab957b5470a0bec8ed96f6034a78657a8b612d24b0314849594b219cea195

CHANGE CONTROL Do not modify the reviewed files after this re-audit. Any source, dependency, feature, configuration, build, upgrade, or redeployment change that can alter behavior requires another review.

Supersedes the source-level conclusions in MSC-MINNIE-AUD-2026-001 only for the exact v1.1 artifact above.

1. Re-audit conclusion

This is a standard SPL-token claim distributor for the official MINNIE mint. The reviewed v1.1 revision corrects the prior exact-balance sealing denial of service without adding a withdrawal, sweep, arbitrary-recipient, admin-delivery, pause, unseal, or allocation-mutation instruction.

The seal instruction now rejects only an underfunded vault. A balance equal to or greater than the registered obligations can be sealed. Any excess is calculated with checked arithmetic and recorded in the DistributionSealed event as both the complete vault balance and surplus amount. The surplus does not increase buyer allocations.

Critical	High	Medium	Low	Informational
0	0	0	3	2

AUDITOR POSITION The source-level repair is accepted. This is not yet a deployed-binary certification: the production SBF build, feature flags, ProgramData account, binary hash, and upgrade authority must still be verified before public Mainnet attestation.

2. Remediation verification

Prior item	v1.1 change	Re-audit status
M-01: exact-balance seal griefing	Changed vault.amount == committed to vault.amount >= committed; underfunding still fails.	Remediated
Surplus transparency	Seal event records committed, complete vault balance, and surplus atoms.	Verified
Privilege expansion risk	No token recovery, withdrawal, sweep, arbitrary delivery, unseal, or admin-claim path added.	No expansion observed
Dust-deposit regression	One-atom unsolicited surplus test added and reproduced.	Pass

3. Independent validation

- Supplied suite reproduced with the pinned package manifest: 13 tests passed, 0 failed.
- Independent 250-allocation and 250-claim stress model passed with unsolicited surplus, exact aggregate transfers, and replay-state preservation.
- Official MINNIE mint confirmed: 3sNywBnr8hhjBDchhamd6n2vhCQ6WkZf5oPpoH7dkCbQ, 9 decimals.
- Initializer confirmed: 6j8zqbxDbKaGP9tJR1ZTfsAeax6d46jKiL4DFixmB3Li; Program ID confirmed in Rust and Anchor: 74PdwFTJDreMXSqhLNrfJ4gSTiNhEzYdFTHSajHhes5M.

4. Remaining accepted design risks

L-01 - Trusted off-chain registrar

The program does not independently verify payment transactions, payment amounts, payment recipients, external-sale uniqueness, or individual eligibility for the 10% Bad Badge bonus. The authorized initializer supplies the purchase hash, buyer, base allocation, and bonus allocation. Separate global base and bonus caps remain enforced.

Status: accepted design risk. Maintain deterministic sale-ledger reconciliation, duplicate detection, approval records, and second-person review. Do not describe the purchase hash as an on-chain proof of payment.

L-02 - Shared writable claim counter

Every claim still updates the same distribution account's claim_count and claimed_atoms. Solana will serialize transactions that write-lock this account, which may create contention during a simultaneous claim rush.

Status: accepted for the stated distribution size of approximately 250 allocations, subject to local-validator concurrency testing.

L-03 - Permanent funds and allocation lifecycle

Allocations cannot be corrected or cancelled after registration, and the program has no token sweep or close path. Wrong buyer keys, abandoned allocations, lost wallets, unsolicited post-seal deposits, and surplus recorded at seal may remain locked indefinitely.

Status: accepted policy decision. Claims are intended to remain permanently available. Operational procedures must prevent incorrect registrations.

5. Remaining informational items

I-01 - Rust build reproducibility

The v1.1 package adds a pinned JavaScript package and lockfile, resolving the prior test-packaging gap. A production Cargo.lock is still absent. The exact Rust/Anchor build must generate and preserve it before deployment.

I-02 - Deployment and upgrade authority

The devnet-test feature relaxes the official-mint address check. Production must be built without it. The deployed upgrade authority is outside the source package and can replace audited logic if retained.

6. Mandatory Mainnet deployment gates

- Generate and preserve Cargo.lock using the exact production Rust/Anchor environment.
- Build this exact source revision with devnet-test disabled; record the SBF binary hash and complete build command.
- Run local-validator tests for underfunding, unsolicited dust and larger surplus, cap boundaries, duplicate hashes, wrong buyer, replay, insufficient vault funds, and concurrent claims.
- Verify the deployed Program ID and ProgramData account against the reviewed build.
- Verify the official mint, 9 decimals, initializer, distribution PDA, vault mint and authority, claim-opening timestamp, funded obligation, and surplus before seal.
- Document the upgrade authority. Use a documented multisig or revoke it when operational needs permit.
- Reconcile every buyer, payment-signature hash, base allocation, and bonus entitlement against the final off-chain presale ledger before sealing.

7. Scope exclusions

The following were intentionally outside this source-level re-audit and were not silently skipped:

- Website, MetaMask interface, wallet-connect flow, backend, database, registrar scripts, payment collection, presale economics, and Bad Badge eligibility system.
- Private keys, signer devices, treasury custody, personnel controls, operational security, and legal or regulatory compliance.
- Compiled SBF artifact, IDL-to-binary comparison, reproducible Rust build, fuzzing, formal verification, validator execution, and performance load testing.
- Current Mainnet deployment state, ProgramData contents, upgrade authority, vault balance, allocation ledger, opening timestamp, and live token-account balances.
- Third-party dependency internals beyond how the supplied source calls them.

8. Evidence and exact hashes

File	SHA-256
programs/.../src/lib.rs	336a2def720a737c01109b23887c24a0372f5868cbf4cc0856035a817068c109
programs/.../Cargo.toml	15b3cd7a4e3ad7c9cfc29089ca72471ba6f0e6b6f30381d4f7564fad06fd55b4
Cargo.toml	b42c5dd145be8fbd80183fc9847a75e26de6940c485b631649d749c852559a78
Anchor.toml	1e6014476ba1d0946fa9352c0082b8a45a99ead3513b19828b51b1f276f250c8
model.mjs	a105fdef1719a9a9f5234e6aa8a0af39346c4815c8082251dc0ffb72f0277601
tests/...test.mjs	bf389d7300463679f57e24557237527052863002 6f843201b5b29e392bcbce28
package.json	2388083f9eeb9d0a833fc9e9255f3422c98e65d45309aa25de74360a9fa13fbe
package-lock.json	a0d971399fe61aa937d2924572452b68525a4bcc50acd4ddddd710734b663796e

9. Final statement

M-01 from preliminary report MSC-MINNIE-AUD-2026-001 is remediated in the exact v1.1 source identified above. No new Critical, High, or Medium-severity vulnerability was identified in the changed sealing logic or surrounding claim flow. The three Low-severity design risks remain accepted and documented.

REVIEW INVALIDATION The reviewed files must not be modified after this re-audit. Any behavior-affecting contract or configuration-source change, dependency change, feature change, rebuild, upgrade, or redeployment requires review again.