

AirdropDesk Contract Internal Security Review

BulkAirdropWithFee • Internal engineering review • 12 July 2026

Scope and status

- Scope: Remix single-file contract, OpenZeppelin-source variant, frontend transaction flow, and four deployed EVM contracts.
- Review type: internal engineering review. This is not an independent third-party audit and does not guarantee that the contracts are vulnerability-free.
- The owner and current fee recipient on all reviewed chains is 0xfD148d89eF7D87FFbB18183DbE50EA3baD67FF7c.

Executive summary

- No critical issue was found in the reviewed transfer loop.
- The flow is atomic, uses safe ERC-20 calls, has a reentrancy guard, validates array lengths and zero values, and limits each call to a bounded recipient count.
- The main trust risk is mutable pricing without a user-supplied maximum-fee parameter.

Deployment snapshot

- Ethereum: 0x3FFEB97DABA42CDfeECB1200f190477C991c432b • 0.01 USDC • max 300.
- BNB Chain: 0x1CfF989BF2464586BCfA4Edd0f1CCa791c11006E • 0.01 USDC • max 300.
- Arbitrum: 0x9209618E0b2B1EA085C5d8a3DB613768A9c9de15 • 0.01 USDC • max 300.
- Base: 0xF2b32a7D21827AB3f55182Cf31523E7523bCEdd1 • 0.01 USDC • max 300.

AirdropDesk Contract Internal Security Review

BulkAirdropWithFee • Internal engineering review • 12 July 2026

M-01 • No maximum-fee protection • Medium

- airdropERC20 calculates the service fee when the transaction is mined. The calldata does not bind an expected fee token, maximum service fee, or deadline.
- If the owner changes pricing before inclusion, a user with a large prior allowance can pay more than the frontend preview.
- Recommendation: add maxServiceFee, expectedServiceToken, and deadline parameters in the next deployment.

M-02 • Immediate centralized configuration • Medium

- The owner can immediately change the service token, unit price, fee recipient, and batch limit without a timelock or multisig requirement.
- Recommendation: transfer ownership to a multisig and consider delayed pricing activation.

L-01 • No pause mechanism • Low

- The deployed version cannot pause new calls during an operational incident.
- Recommendation: add a narrowly scoped pause controlled by a multisig.

AirdropDesk Contract Internal Security Review

BulkAirdropWithFee • Internal engineering review • 12 July 2026

L-02 • No accidental-token recovery • Low

- Tokens transferred directly to the contract address cannot be recovered. Normal airdrops do not custody tokens in the contract.
- Recommendation: document this behavior. Any future recovery function should be restricted to a multisig and must not access user allowances.

I-01 • Duplicate direct calls • Informational

- The frontend merges duplicate recipients. Direct contract callers can submit duplicate addresses and are billed per array entry.

I-02 • Non-standard token behavior • Informational

- Fee-on-transfer, rebasing, blocked-address, or callback-enabled tokens may deliver different balances or revert.
- Recommendation: test unusual tokens before large distributions.

Controls that passed

- nonReentrant protects the fee and distribution flow.
- Any failed fee or recipient transfer reverts the entire transaction.
- Zero checks, length checks, checked arithmetic, and a maximum recipient cap are present.
- The owner has no arbitrary withdrawal, arbitrary user transfer, proxy, delegatecall, or upgrade function.
- The source compiles with Solidity 0.8.34 and optimization disabled.

AirdropDesk Contract Internal Security Review

BulkAirdropWithFee • Internal engineering review • 12 July 2026

Upgradeability

- The four deployed contracts are not upgradeable. There is no proxy, implementation address, delegatecall, or upgrade function.
- Changing executable logic requires a new deployment and a website configuration update.

Administrator permissions

- Owner can call setPricing to change the service token, unit price, and fee recipient.
- Owner can set maxRecipientsPerTx between 1 and 500.
- Owner can transfer ownership to another non-zero address.
- Owner cannot initiate an airdrop from a user wallet, pull tokens without a user-initiated contract call, or replace deployed bytecode.

Recommended next version

- Add maximum-fee, expected-token, and deadline protections.
- Use multisig ownership and delayed pricing updates.
- Add a narrowly scoped pause mechanism.
- Add tests for mutable pricing, malicious token callbacks, fee-on-transfer tokens, and maximum-batch gas limits.

References

- Full findings: AIRDROPDESK-CONTRACT-AUDIT.md.
- Addresses and constructor arguments: CONTRACT-VERIFICATION.md.
- Verification source: contracts/BulkAirdropWithFee.remix.sol.