Ika Mdrop Audit

audited by Asymptotic

August 12, 2025

Summary

Asymptotic conducted a security audit of Ika's Mdrop contract. The audit identified 1 low-severity and 1 advisory issues. The low-severity issue has been remediated.

- Initial commit: `https://github.com/dwallet-labs/ika-drop/commit/ad2c62f`
- Final commit: `https://github.com/dwallet-labs/ika-drop/commit/43740d9`
- Audited directories:
  `./contracts/human-id`
  `./contracts/ika`
  `./contracts/ika_distribution`
  `./contracts/sbt-verifier`

Legend

Issue severity

- **Critical** — Vulnerabilities which allow account takeovers or stealing significant funds, along with being easy to exploit.
- **High** — Vulnerabilities which either can have significant impact but are hard to exploit, or are easy to exploit but have more limited impact.
- **Medium** — Moderate risks with notable but limited impact.
- **Low** — Minor issues with minimal security implications.
- **Advisory** — Informational findings for security/code improvements.

Legal Disclaimer

Terms and Conditions and Liability

This report is subject to the terms and conditions—including liability limitations—established between Asymptotic and the paying entity. By sharing code with Asymptotic, developers acknowledge and agree to these conditions.

Scope

This security audit report focuses specifically on reviewing the Move smart contract code. The audit does not analyze or make any claims about other components of the system, including but not limited to:

- Frontend applications and user interfaces
- Backend services and infrastructure
- Off-chain components and integrations
- Deployment procedures and operational security
- Third-party dependencies and external services

Limitations

The findings and recommendations in this report are limited to the Move code implementation and its immediate interactions within the Sui blockchain environment.

L-1: Insecure coin metadata handling

Severity: Low

Description

The metadata for the IKA coin is handled insecurely during initialization. The module uses transfer::public_share_object(coin_metadata) instead of transfer::public_freeze_object(coin_metadata) when creating a new currency.

Remediation

✓ **Commit:** 476350e

A-1: Incomplete checks in set_config

Severity: Advisory

Description

If set_config is intended to modify the config parameters after the drop is already in progress (config.start_time_ms ¡= clock.timestamp_ms()), then maybe end_time_ms should be in the future, to avoid abruptly ending the drop.

Remediation

Acknowledged: The developers acknowledged they do not intend to call set_config while the drop is in progress.

About the Auditor

Asymptotic provides a white-glove, formal-verification-based auditing service for Sui smart contracts.

Lead Auditor
Andrei Stefanescu – Chief Scientist

- Led verification of AWS cryptographic algorithms using SAW at Galois
- Created first Ethereum smart contract verification tool
- Three-time International Math Olympiad silver medalist
- PhD in Computer Science from UIUC with David J. Kuck Outstanding Thesis Award
- ACM SIGPLAN Distinguished Paper Award at OOPSLA 2016
- Pioneered K Framework for programming language semantics and verification

Auditor
Dmytro Sotnyk

- Developed cross-chain bridges between Ethereum and Kadena, and reconstructed Hyperlane protocol using Pact
- Conducted smart contract audits, developed audit methodologies, and researched vulnerabilities at Hacken
- Built backend solutions for Hedera Hashgraph and Solidity-based smart contracts with Web3 wallet integrations
- Proficient in Solidity, Pact, TypeScript, Python, and blockchain testing tools (Echidna, Slither)