

# SSA Security Scan Report

## Target Information

Target: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3

Kind: wallet

Scan Level: L3

Timestamp: 2026-01-11T20:02:36.984Z

## Summary

Verdict: FAIL

Risk Score: 74/100

Security Verified: No

## Severity Summary

Critical: 0

High: 30

Medium: 9

Low: 1

Info: 2

## Findings

### HIGH (30)

ID: SVSSA-MOVE-VIEW-001

Title: Missing Required View Functions

Confidence: 100%

Description: Failed to fetch 1 required view function(s): pool\_stats. This prevents complete security analysis.

Recommendation: Ensure all required view functions are available and accessible. Check RPC endpoint connectivity and module deployment status.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v10

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v10

ID: SVSSA-MOVE-VIEW-001

Title: Missing Required View Functions

Confidence: 100%

Description: Failed to fetch 1 required view function(s): pool\_stats. This prevents complete security analysis.

Recommendation: Ensure all required view functions are available and accessible. Check RPC endpoint connectivity and module deployment status.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v10

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v10

ID: SVSSA-MOVE-VIEW-001

Title: Missing Required View Functions

Confidence: 100%

Description: Failed to fetch 1 required view function(s): pool\_stats. This prevents complete security analysis.

Recommendation: Ensure all required view functions are available and accessible. Check RPC endpoint connectivity and module deployment status.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v11

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v11

ID: SVSSA-MOVE-VIEW-001

Title: Missing Required View Functions

Confidence: 100%

Description: Failed to fetch 1 required view function(s): pool\_stats. This prevents complete security analysis.

Recommendation: Ensure all required view functions are available and accessible. Check RPC endpoint connectivity and module deployment status.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v11

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v11

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v12

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v12

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v13

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v13

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v14

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v14

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v15

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v15

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v16

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v16

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v17

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v17

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v18

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v18

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v19

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v19

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v23

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v23

ID: SVSSA-MOVE-VIEW-001

Title: Missing Required View Functions

Confidence: 100%

Description: Failed to fetch 2 required view function(s): pool\_stats, total\_staked. This prevents complete security analysis.

Recommendation: Ensure all required view functions are available and accessible. Check RPC endpoint connectivity and module deployment status.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::jackpot\_svl

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::jackpot\_svl

ID: SVSSA-MOVE-VIEW-001

Title: Missing Required View Functions

Confidence: 100%

Description: Failed to fetch 2 required view function(s): pool\_stats, total\_staked. This prevents complete security analysis.

Recommendation: Ensure all required view functions are available and accessible. Check RPC endpoint connectivity and module deployment status.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::jackpot\_svl

ID: SVSSA-MOVE-VIEW-QUEUE-MISSING

Title: Missing Queue Capability

Confidence: 100%

Description: Neither v24 nor legacy queue views are available. Queue inspection capabilities are missing.

Recommendation: Verify module deployment and ensure queue view functions are available.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::jackpot\_svl

## MEDIUM (9)

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v14

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v15

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v16

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v17

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v18

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v19

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v23

ID: SVSSA-MOVE-006

Title: Potential Unbounded Loops in Entry Functions

Confidence: 50%

Description: Detected loop-related patterns in bytecode strings. If entry functions iterate over user-controlled vectors without bounds, this may lead to DoS attacks or excessive gas consumption.

Recommendation: Verify that loop bounds are properly enforced and consider adding maximum iteration limits.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v24

ID: SVSSA-MOVE-009

Title: External Dependency/Oracle Usage Without Clear Bounds

Confidence: 60%

Description: Detected oracle/external dependency patterns (price) but limited bounds checking hints. Oracle manipulation or stale data can lead to financial losses.

Recommendation: Verify that oracle values are bounded (min/max) and consider adding staleness checks and multiple oracle sources.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::jackpot\_svl

## LOW (1)

ID: SVSSA-MOVE-007

Title: Missing Event Emissions for Sensitive Operations

Confidence: 50%

Description: Detected sensitive operations (mint/withdraw/admin/upgrade) but no clear event emission patterns found in bytecode/source. Events are important for off-chain monitoring and transparency.

Recommendation: Emit events for all sensitive operations (transfers, mints, burns, admin actions) to enable off-chain monitoring and improve transparency.

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v24

## INFO (2)

ID: SVSSA-MOVE-005-INFO

Title: Expected Staking Outflow Pattern

Confidence: 80%

Description: Entry function "view\_withdraw\_requests" matches expected staking outflow pattern. Verify access control is properly enforced via request/fulfill pattern.

Recommendation: Ensure this function uses proper access control (e.g., request/fulfill pattern, signer verification).

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v24

ID: SVSSA-MOVE-005-INFO

Title: Expected Staking Outflow Pattern

Confidence: 80%

Description: Entry function "view\_claim\_requests" matches expected staking outflow pattern. Verify access control is properly enforced via request/fulfill pattern.

Recommendation: Ensure this function uses proper access control (e.g., request/fulfill pattern, signer verification).

Module: 0xd1c64ad544a0fe534f4e2641a4515b6a0629b26c29f36d6423014b192b7abee3::staking\_v24