

# SSA Security Scan Report

## Target Information

Target: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f

Kind: wallet

Scan Level: L2

Timestamp: 2026-01-11T23:49:00.448Z

## Summary

Verdict: PASS

Risk Score: 4/100

Security Verified: No

## Severity Summary

Critical: 0

High: 0

Medium: 6

Low: 0

Info: 0

## Findings

### MEDIUM (6)

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: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f::vaultpay\_presale

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: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f::vaultpay\_presale\_v2

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: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f::vaultpay\_presale\_v3

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: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f::vaultpay\_subscriptions

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: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f::vaultpay\_subscriptions\_v2

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: 0xdf015c749bea2080c9096f1655ab4c40cfe0782b52520a48fb3f56d6a08f436f::vaultpay\_subscriptions\_v3