SSA Security Scan Report

Target Information

Target: 0x9176f70f125199a3e3d5549ce795a8e906eed75901d535ded623802f15ae3637
Kind: wallet
Scan Level: L3
Timestamp: 2026-01-11T05:42:45.631Z

Summary

Verdict: PASS
Risk Score: 0/100
Badge: SSA · Wallet Verified
Expires: 2026-01-18T05:42:45.632Z

Severity Summary

Critical: 0
High: 0
Medium: 0
Low: 0
Info: 0

Supra Pulse Intelligence (Integrated)

Supra Pulse report integrated and attached.
Filename: supra_pulse.pdf
SHA256: 424266ce3546b372c4f6ca451b0087936ceff5c779c7396a48c6f9bfe43a68d4
Kind: PDF

SSA Security Scan Report

Target Information
Target: 0x9176f70f125199a3e3d5549ce795a8e906eed75901d535ded623802f15ae3637::cdp_multi
Kind: coin
Scan Level: L3
Timestamp: 2026-01-11T05:42:45.909Z

Summary
Verdict: INCONCLUSIVE
Risk Score: 66/100
Security Verified: No

Severity Summary
Critical: 0
High: 4
Medium: 3
Low: 1
Info: 0

Findings
HIGH (4)
ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control
Confidence: 80%
Description: Module "events" contains exposed function "emit_debt_minted_event" matching dangerous patterns (mint) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control
Confidence: 80%
Description: Module "cdp_multi" contains exposed function "deposit_or_mint" matching dangerous patterns (mint) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control
Confidence: 80%
Description: Module "vault_core" contains exposed function "max_mint" matching dangerous patterns (mint) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control
Confidence: 80%
Description: Module "vault_core" contains exposed function "preview_mint" matching dangerous patterns (mint) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

MEDIUM (3)
ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control

Confidence: 80%
Description: Module "events" contains exposed function "err_not_admin" matching dangerous patterns (admin) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control
Confidence: 80%
Description: Module "vault_core" contains exposed function "pause" matching dangerous patterns (pause) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

ID: COIN-SEC-001
Title: Dangerous Function Without Clear Access Control
Confidence: 80%
Description: Module "vault_core" contains exposed function "unpause" matching dangerous patterns (pause) but lacks clear gating mechanisms (admin/owner checks, capability verification).
Recommendation: Implement strict access control checks (e.g., `only_admin`, `only_owner`, capability checks) for functions that modify token state or configuration.

LOW (1)
ID: COIN-META-001
Title: Missing or Incomplete Metadata
Confidence: 90%
Description: Coin metadata is missing or incomplete. Missing: symbol, decimals, totalSupply
Recommendation: Ensure all standard coin metadata fields are available via view functions or indexer.

Supra Pulse Intelligence (Integrated)

Supra Pulse report integrated and attached.
Filename: supra_pulse.pdf
SHA256: 424266ce3546b372c4f6ca451b0087936ceff5c779c7396a48c6f9bfe43a68d4
Kind: PDF