OSVM Security Audit Report

Comprehensive Security Assessment

Generated: 2025-08-01 22:20:32 UTC

Version: 0.4.4

Security Score: 40.68096160888672/100

Compliance Level: Critical

1. Executive Summary

This report presents the results of a comprehensive security audit conducted on the OSVM (Open SVM) CLI application. The audit identified 793 findings across various security domains.

Metric	Value
Total Findings	793
Critical	197
High	344
Medium	80
Low	3
Info	169
Security Score	40.68096160888672/100
Compliance Level	Critical

⚠️ **This audit identified 541 critical or high severity findings that require immediate attention.**

2. System Information

Component	Version
Rust	rustc 1.87.0 (17067e9ac 2025-05-09)
Solana	Not installed
OS	linux x86_64
Architecture	x86_64

3. Security Findings

3.1. Configuration (1 findings)

3.1.1. OSVM-002 - Solana CLI not installed

Severity: High **Category:** Configuration

CVSS Score: 7.5

Description: Solana CLI is required for OSVM operations

Impact: General security concern requiring assessment

Recommendation: Install Solana CLI using the official installer

References:

- https://docs.solana.com/running-validator/validator-start

3.2. Cryptography (163 findings)

3.2.1. OSVM-CRYPTO-f7bc881910702778 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.2. OSVM-CRYPTO-546bcf7db59b7255 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.3. OSVM-CRYPTO-0919b079cddb0d08 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.4. OSVM-CRYPTO-5cfb051bd16dbdea - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.5. OSVM-CRYPTO-12256568ffa95646 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.6. OSVM-CRYPTO-b5c92c2d35a6aa23 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.7. OSVM-CRYPTO-54b3a86388b76c62 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File svmai-token

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: svmai-token:svmai-token

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.8. OSVM-CRYPTO-3f49f73c4df44be0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.9. OSVM-CRYPTO-b9be119638d87d18 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.10. OSVM-CRYPTO-8aa4e605899f7aa6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.11. OSVM-CRYPTO-332db3a4ea224f4d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.12. OSVM-CRYPTO-e03a77f6422d29fd - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.13. OSVM-CRYPTO-731179ac715bf46a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.14. OSVM-CRYPTO-6927a082bb3dba42 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.15. OSVM-CRYPTO-54dded77b1e6d303 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.16. OSVM-CRYPTO-0a7dc131f9983032 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.17. OSVM-CRYPTO-4bf8d9b95e10a642 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.18. OSVM-CRYPTO-628870345ac14c47 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.19. OSVM-CRYPTO-a1fdae9bdad8bdf7 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.20. OSVM-CRYPTO-63368d4cf8575a7f - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.21. OSVM-CRYPTO-b98cd23a031725b1 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.22. OSVM-CRYPTO-3768812dff0d3fc5 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.23. OSVM-CRYPTO-cae1a1fed252b2e0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.24. OSVM-CRYPTO-75242467cd3b994b - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.25. OSVM-CRYPTO-e072034b1cf6eb84 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.26. OSVM-CRYPTO-841a95f9ebac03cf - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.27. OSVM-CRYPTO-1e5edfb59abedc82 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.28. OSVM-CRYPTO-b6a2a81c185a7dbf - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.29. OSVM-CRYPTO-5e672147707bc934 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.30. OSVM-CRYPTO-725230a021f6dd16 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.31. OSVM-CRYPTO-545e4231f4aa9349 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.32. OSVM-CRYPTO-e2d6cb4ddca0f1b0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.33. OSVM-CRYPTO-9ba14589e28c0b2c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.34. OSVM-CRYPTO-ebbae05e1c8f0c7d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.35. OSVM-CRYPTO-6d6acdbcdb8aac6d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.36. OSVM-CRYPTO-721edd285e83acbc - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.37. OSVM-CRYPTO-cd0f9e1fdb839e02 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.38. OSVM-CRYPTO-ec28fd14f84c63fa - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.39. OSVM-CRYPTO-4d232641ba85a927 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.40. OSVM-CRYPTO-d6ee48449f4b5bbe - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.41. OSVM-CRYPTO-0e1c13b326c0fd10 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.42. OSVM-CRYPTO-50651d4a4fe74592 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.43. OSVM-CRYPTO-0527345219c53266 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.44. OSVM-CRYPTO-326ef1fb4aa224d9 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.45. OSVM-CRYPTO-aa555f2254618265 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.46. OSVM-CRYPTO-2bdab565b24c52d0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.47. OSVM-CRYPTO-0bbba94c7b5f05c4 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.48. OSVM-CRYPTO-7e89fb3e12fa5975 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.49. OSVM-CRYPTO-1028feb859ec1ad5 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.50. OSVM-CRYPTO-e418d8ef77a94e10 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.51. OSVM-CRYPTO-6936937e8c22380f - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.52. OSVM-CRYPTO-f8ca25d23b075345 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.53. OSVM-CRYPTO-4806ad5564f32272 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.54. OSVM-CRYPTO-7121e5d7187ecb06 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.55. OSVM-CRYPTO-318598db35bc1523 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.56. OSVM-CRYPTO-e5e8b45dc7c36914 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.57. OSVM-CRYPTO-1a4e92245bf522a6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.58. OSVM-CRYPTO-1e18f48872ee62ae - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.59. OSVM-CRYPTO-2f980010885f134c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.60. OSVM-CRYPTO-002c48dd22cb2f7d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.61. OSVM-CRYPTO-e346ce8fa6865473 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.62. OSVM-CRYPTO-a61f91399c6de6c6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.63. OSVM-CRYPTO-7cf6087ecb5daa5a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.64. OSVM-CRYPTO-c2b46030b2989924 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.65. OSVM-CRYPTO-4899379294bb035a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.66. OSVM-CRYPTO-6ff181a9ae9a4dc7 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.67. OSVM-CRYPTO-229c9f6864ec7d1d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File agent-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: agent-registry:agent-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.68. OSVM-CRYPTO-b80dd2972c317f9b - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.69. OSVM-CRYPTO-f2428b32bfb25eb4 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.70. OSVM-CRYPTO-05b98f43176a3dc7 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.71. OSVM-CRYPTO-7e44373e29483791 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.72. OSVM-CRYPTO-9572b9ad92bad04a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.73. OSVM-CRYPTO-e24baeb54c95c617 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.74. OSVM-CRYPTO-aa664967fbc077b8 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.75. OSVM-CRYPTO-332a5e391c08d7b6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File common

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: common:common

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.76. OSVM-CRYPTO-b1deb6e3311b9043 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.77. OSVM-CRYPTO-23bdb8931625e94c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.78. OSVM-CRYPTO-239be6b2617a610a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.79. OSVM-CRYPTO-3146a191f2a9f57f - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.80. OSVM-CRYPTO-ddaf5007dae74f69 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.81. OSVM-CRYPTO-e03dc645c9c64a6c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.82. OSVM-CRYPTO-c8e21ec3459ca470 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.83. OSVM-CRYPTO-af80be5ef1a68d14 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.84. OSVM-CRYPTO-9e632bf9dfd43181 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.85. OSVM-CRYPTO-2b4da1cd85a1c506 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.86. OSVM-CRYPTO-6c39b6da17671f74 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.87. OSVM-CRYPTO-c86096c2774fd8a5 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.88. OSVM-CRYPTO-87e9e0c854a0481e - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.89. OSVM-CRYPTO-1c6ad52f6db6c585 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.90. OSVM-CRYPTO-ae1e19187021e6f6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.91. OSVM-CRYPTO-5642101702c78921 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.92. OSVM-CRYPTO-70ad5056fc60fba0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.93. OSVM-CRYPTO-adee51f77e573514 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.94. OSVM-CRYPTO-efd90927ec86c08d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.95. OSVM-CRYPTO-a5ea0581efa7f886 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.96. OSVM-CRYPTO-72d49c0fc6402fe0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.97. OSVM-CRYPTO-72a2280220ece260 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.98. OSVM-CRYPTO-8e25eff943320c42 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.99. OSVM-CRYPTO-d6f58dda9cdf4757 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.100. OSVM-CRYPTO-da24831c2c527c5f - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.101. OSVM-CRYPTO-f1404343c5c0706c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.102. OSVM-CRYPTO-b4ff47681850473c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.103. OSVM-CRYPTO-7c83df6daac3c5d9 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.104. OSVM-CRYPTO-5142f88254ef69ce - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.105. OSVM-CRYPTO-7f942734d2821284 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.106. OSVM-CRYPTO-e1cc4d8efd89aa5a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.107. OSVM-CRYPTO-1a2c4c2bc45d534a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.108. OSVM-CRYPTO-9d848f60ccbae524 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.109. OSVM-CRYPTO-0143a56233eba422 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.110. OSVM-CRYPTO-d773263112aa0448 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.111. OSVM-CRYPTO-1eb96025708c5cf1 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.112. OSVM-CRYPTO-299f515f6a558b7c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.113. OSVM-CRYPTO-d8b29744c770b7f4 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.114. OSVM-CRYPTO-dbcece043d53bf5d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.115. OSVM-CRYPTO-59327d04a56b1e6c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.116. OSVM-CRYPTO-3a1ebde68d133a5d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.117. OSVM-CRYPTO-d97cf1dc14bd663e - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.118. OSVM-CRYPTO-1f0121db396dc9dd - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.119. OSVM-CRYPTO-15082c5e7181ad26 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.120. OSVM-CRYPTO-0a1d62785f9d92cb - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.121. OSVM-CRYPTO-6e9ffc4e1dc1acba - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.122. OSVM-CRYPTO-9ec57b0378445b4c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.123. OSVM-CRYPTO-11b53d0ab4eabd5e - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.124. OSVM-CRYPTO-e7b68e6ed251a6ee - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.125. OSVM-CRYPTO-98b21edf35f9adc4 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.126. OSVM-CRYPTO-73c1a9d344487da9 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.127. OSVM-CRYPTO-0c64920adf701301 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.128. OSVM-CRYPTO-f0c6e4fe8a83221c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.129. OSVM-CRYPTO-ff347f7d36fa4ac6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.130. OSVM-CRYPTO-b4a61863641619c9 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.131. OSVM-CRYPTO-64578f45bc599fbc - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.132. OSVM-CRYPTO-4932a39c16890955 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.133. OSVM-CRYPTO-42914efce7f25a4b - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.134. OSVM-CRYPTO-98635ad4c0ec2c25 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.135. OSVM-CRYPTO-08fabfb5be013364 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.136. OSVM-CRYPTO-e4d9db39ae90f5e0 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.137. OSVM-CRYPTO-58ddc14607e78bde - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.138. OSVM-CRYPTO-11ecfd0a13ff05bb - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.139. OSVM-CRYPTO-4f2f8e67e5eb34cf - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.140. OSVM-CRYPTO-8ef6a29002f25f0e - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.141. OSVM-CRYPTO-db2d2995eb744633 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.142. OSVM-CRYPTO-93897b30337da16d - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.143. OSVM-CRYPTO-6f78155e8968e524 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.144. OSVM-CRYPTO-7e6f04ba337e7314 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.145. OSVM-CRYPTO-fbcb164bc9303406 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.146. OSVM-CRYPTO-7d3de41f04b4ab38 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.147. OSVM-CRYPTO-4750fb462f2781c2 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.148. OSVM-CRYPTO-a06d059f6c0392de - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.149. OSVM-CRYPTO-97689d021bc588cc - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.150. OSVM-CRYPTO-cd19e86c948b559c - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.151. OSVM-CRYPTO-19985928a1696e1e - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.152. OSVM-CRYPTO-fb798789d882c5a5 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.153. OSVM-CRYPTO-d9b844bb59d9f506 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.154. OSVM-CRYPTO-a731ff334d25ddc6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.155. OSVM-CRYPTO-af42660c74a6d5c1 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.156. OSVM-CRYPTO-9a91f532b268b43e - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.157. OSVM-CRYPTO-65bb0d8efc95b95a - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.158. OSVM-CRYPTO-e8b5ebdd038ed4d6 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.159. OSVM-CRYPTO-c1f6d1c9d3cd0adc - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.160. OSVM-CRYPTO-7e650e0d2c099d6b - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.161. OSVM-CRYPTO-f8c7659df3f40d78 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.162. OSVM-CRYPTO-7ba790e1b7b72161 - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.2.163. OSVM-CRYPTO-aaf5635db470831b - Hardcoded secret detected

Severity: High **Category:** Cryptography **CWE ID:** CWE-798 **CVSS Score:** 8

Description: File rust

Impact: Exposed secrets could lead to unauthorized access

Recommendation: Remove hardcoded secrets and use environment variables or secure key management

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/798.html

3.3. Dependencies (4 findings)

3.3.1. OSVM-001 - Update available: rust

Severity: Medium **Category:** Dependencies

CVSS Score: 5

Description: An update is available for rust

Impact: General security concern requiring assessment

Recommendation: Run system updates

References:

- https://rustsec.org/
- https://docs.rs/cargo-audit/

3.3.2. OSVM-100 - Dependency vulnerability scanning unavailable

Severity: Low **Category:** Dependencies **CWE ID:** CWE-1104 **CVSS Score:** 2

Description: cargo-audit is not installed or failed to run, dependency vulnerabilities cannot be checked

Impact: Unknown vulnerabilities in dependencies may exist

Recommendation: Install cargo-audit with 'cargo install cargo-audit' and run regular dependency scans

References:

- https://crates.io/crates/cargo-audit
- https://rustsec.org/

3.3.3. OSVM-ae65ee6118b4e9e5 - External path dependency: aeamcp-common

Severity: Low **Category:** Dependencies **CWE ID:** CWE-426 **CVSS Score:** 3

Description: Dependency 'aeamcp-common' references path outside project: ../common

Impact: External path dependencies may not be version controlled

Recommendation: Consider using published crate for dependency 'aeamcp-common'

Code Location: Cargo.toml

References:

- https://doc.rust-lang.org/cargo/reference/specifying-dependencies.html#specifying-path-dependencies

3.3.4. OSVM-44d64b2438a7da19 - External path dependency: aeamcp-common

Severity: Low **Category:** Dependencies **CWE ID:** CWE-426 **CVSS Score:** 3

Description: Dependency 'aeamcp-common' references path outside project: ../common

Impact: External path dependencies may not be version controlled

Recommendation: Consider using published crate for dependency 'aeamcp-common'

Code Location: Cargo.toml

References:

- https://doc.rust-lang.org/cargo/reference/specifying-dependencies.html#specifying-path-dependencies

3.4. Error Handling (11 findings)

3.4.1. OSVM-734b0519b680203c - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File svmai-token

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: svmai-token:svmai-token

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html

- https://cwe.mitre.org/data/definitions/248.html

3.4.2. OSVM-b0aacc351c386576 - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File agent-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: agent-registry:agent-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.3. OSVM-0979e2e4a1e785dc - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File agent-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: agent-registry:agent-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.4. OSVM-1900fc2b158cf429 - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File agent-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: agent-registry:agent-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.5. OSVM-f14221d73edbe829 - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File agent-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: agent-registry:agent-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.6. OSVM-6254ed304579461d - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File agent-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: agent-registry:agent-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.7. OSVM-432fcf368ea0ed95 - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File common

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: common:common

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.8. OSVM-72cb5c634f7d90ca - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File mcp-server-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.9. OSVM-b461ce88aae1a583 - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File mcp-server-registry

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.10. OSVM-2da1f15d9d3e60dc - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File rust

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: rust:rust

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.4.11. OSVM-3eef3211db68bd62 - Excessive unwrap/expect usage

Severity: Medium **Category:** Error Handling **CWE ID:** CWE-248 **CVSS Score:** 4

Description: File rust

Impact: Application crashes due to unhandled panics, potential denial of service

Recommendation: Replace unwrap/expect with proper error handling using match or if let patterns

Code Location: rust:rust

References:

- https://doc.rust-lang.org/book/ch09-00-error-handling.html
- https://cwe.mitre.org/data/definitions/248.html

3.5. Memory Safety (1 findings)

3.5.1. OSVM-08961f9a5861c9b8 - Unsafe code block detected

Severity: Medium **Category:** Memory Safety **CWE ID:** CWE-119 **CVSS Score:** 5.5

Description: File rust

Impact: Potential memory safety violations and buffer overflows

Recommendation: Review unsafe code blocks carefully, ensure proper bounds checking and memory management

Code Location: rust:rust

References:

- https://doc.rust-lang.org/book/ch19-01-unsafe-rust.html
- https://cwe.mitre.org/data/definitions/119.html

3.6. Network Security (13 findings)

3.6.1. OSVM-NET-98bca3932cc50686 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.2. OSVM-NET-bd0d1c90a8a23429 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.3. OSVM-NET-c7b63e5bd464e030 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.4. OSVM-NET-b45e89294a488fff - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.5. OSVM-NET-c41575f1d7ced39b - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.6. OSVM-NET-5fa83835c9fa8d02 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.7. OSVM-NET-6f76d58dd7ac7e00 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html

- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.8. OSVM-NET-7571b913226c32fa - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.9. OSVM-NET-7610c979e81ca22a - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.10. OSVM-NET-9eb76631e463df0a - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.11. OSVM-NET-1078fd21c856e01c - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.12. OSVM-NET-632423af446ed156 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.6.13. OSVM-NET-a02cb04624073429 - Insecure HTTP usage detected

Severity: Medium **Category:** Network Security **CWE ID:** CWE-319 **CVSS Score:** 5

Description: File rust

Impact: Data transmitted in plain text, susceptible to interception

Recommendation: Use HTTPS for all external network communications

Code Location: rust:rust

References:

- https://cwe.mitre.org/data/definitions/319.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

3.7. Security (169 findings)

3.7.1. OSVM-101 - Dependency lock file present

Severity: Info **Category:** Security

Description: Project uses Cargo.lock for reproducible builds

Impact: Good practice: Lock files ensure reproducible builds and prevent supply chain attacks

Recommendation: Keep Cargo.lock in version control for reproducible builds

Code Location: Cargo.lock

References:

- https://doc.rust-lang.org/cargo/guide/cargo-toml-vs-cargo-lock.html

3.7.2. OSVM-102 - Comprehensive testing infrastructure

Severity: Info **Category:** Security

Description: Project includes testing infrastructure

Impact: Good practice: Comprehensive testing reduces security vulnerabilities

Recommendation: Continue maintaining comprehensive test coverage

Code Location: tests/

References:

- https://doc.rust-lang.org/book/ch11-00-testing.html

3.7.3. OSVM-103 - Project documentation present

Severity: Info **Category:** Security

Description: Project includes comprehensive documentation

Impact: Good practice: Good documentation helps users understand security implications

Recommendation: Keep documentation up to date with security considerations

Code Location: README.md

References:

- https://owasp.org/www-project-application-security-verification-standard/

3.7.4. OSVM-104 - Automated CI/CD pipeline

Severity: Info **Category:** Security

Description: Project uses automated CI/CD with GitHub Actions

Impact: Good practice: Automated CI/CD improves security through consistent builds and testing

Recommendation: Continue using automated CI/CD for security and quality assurance

Code Location: .github/workflows/

References:

- https://owasp.org/www-project-devsecops-toolkit/

3.7.5. OSVM-105 - Comprehensive .gitignore configuration

Severity: Info **Category:** Security

Description: Project properly excludes sensitive files from version control

Impact: Good practice: Proper .gitignore prevents accidental secret commits

Recommendation: Continue maintaining comprehensive .gitignore patterns

Code Location: .gitignore

References:

- https://git-scm.com/docs/gitignore

3.7.6. OSVM-106 - Security documentation present

Severity: Info **Category:** Security

Description: Project includes security-related documentation: rust_security_audit_2025.pdf

Impact: Good practice: Security documentation helps maintain secure development practices

Recommendation: Keep security documentation up to date

Code Location: rust_security_audit_2025.pdf

References:

- https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

3.7.7. OSVM-107 - Professional project structure: tests directory

Severity: Info **Category:** Security

Description: Project includes tests directory for comprehensive development

Impact: Good practice: Complete project structure supports secure development lifecycle

Recommendation: Continue maintaining professional project organization

Code Location: tests/

References:

- https://doc.rust-lang.org/cargo/guide/project-layout.html

3.7.8. OSVM-108 - Professional project structure: docs directory

Severity: Info **Category:** Security

Description: Project includes docs directory for comprehensive development

Impact: Good practice: Complete project structure supports secure development lifecycle

Recommendation: Continue maintaining professional project organization

Code Location: docs/

References:

- https://doc.rust-lang.org/cargo/guide/project-layout.html

3.7.9. OSVM-109 - Explicit dependency versioning

Severity: Info **Category:** Security

Description: Project explicitly versions 9 dependencies

Impact: Good practice: Explicit versioning prevents supply chain attacks and ensures reproducible builds

Recommendation: Continue explicitly versioning all dependencies

Code Location: Cargo.toml

References:

- https://doc.rust-lang.org/cargo/reference/specifying-dependencies.html

3.7.10. OSVM-110 - Security best practice indicator 1

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.11. OSVM-111 - Security best practice indicator 2

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.12. OSVM-112 - Security best practice indicator 3

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.13. OSVM-113 - Security best practice indicator 4

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.14. OSVM-114 - Security best practice indicator 5

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.15. OSVM-115 - Security best practice indicator 6

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.16. OSVM-116 - Security best practice indicator 7

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.17. OSVM-117 - Security best practice indicator 8

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.18. OSVM-118 - Security best practice indicator 9

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.19. OSVM-119 - Security best practice indicator 10

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.20. OSVM-120 - Security best practice indicator 11

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.21. OSVM-121 - Security best practice indicator 12

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.22. OSVM-122 - Security best practice indicator 13

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.23. OSVM-123 - Security best practice indicator 14

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.24. OSVM-124 - Security best practice indicator 15

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.25. OSVM-125 - Security best practice indicator 16

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.26. OSVM-126 - Security best practice indicator 17

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.27. OSVM-127 - Security best practice indicator 18

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.28. OSVM-128 - Security best practice indicator 19

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.29. OSVM-129 - Security best practice indicator 20

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.30. OSVM-130 - Security best practice indicator 21

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.31. OSVM-131 - Security best practice indicator 22

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.32. OSVM-132 - Security best practice indicator 23

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.33. OSVM-133 - Security best practice indicator 24

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.34. OSVM-134 - Security best practice indicator 25

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.35. OSVM-135 - Security best practice indicator 26

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.36. OSVM-136 - Security best practice indicator 27

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.37. OSVM-137 - Security best practice indicator 28

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.38. OSVM-138 - Security best practice indicator 29

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.39. OSVM-139 - Security best practice indicator 30

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.40. OSVM-140 - Security best practice indicator 31

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.41. OSVM-141 - Security best practice indicator 32

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.42. OSVM-142 - Security best practice indicator 33

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.43. OSVM-143 - Security best practice indicator 34

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.44. OSVM-144 - Security best practice indicator 35

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.45. OSVM-145 - Security best practice indicator 36

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.46. OSVM-146 - Security best practice indicator 37

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.47. OSVM-147 - Security best practice indicator 38

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.48. OSVM-148 - Security best practice indicator 39

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.49. OSVM-149 - Security best practice indicator 40

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.50. OSVM-150 - Security best practice indicator 41

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.51. OSVM-151 - Security best practice indicator 42

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.52. OSVM-152 - Security best practice indicator 43

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.53. OSVM-153 - Security best practice indicator 44

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.54. OSVM-154 - Security best practice indicator 45

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.55. OSVM-155 - Security best practice indicator 46

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.56. OSVM-156 - Security best practice indicator 47

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.57. OSVM-157 - Security best practice indicator 48

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.58. OSVM-158 - Security best practice indicator 49

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.59. OSVM-159 - Security best practice indicator 50

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.60. OSVM-160 - Security best practice indicator 51

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.61. OSVM-161 - Security best practice indicator 52

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.62. OSVM-162 - Security best practice indicator 53

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.63. OSVM-163 - Security best practice indicator 54

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.64. OSVM-164 - Security best practice indicator 55

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.65. OSVM-165 - Security best practice indicator 56

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.66. OSVM-166 - Security best practice indicator 57

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.67. OSVM-167 - Security best practice indicator 58

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.68. OSVM-168 - Security best practice indicator 59

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.69. OSVM-169 - Security best practice indicator 60

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.70. OSVM-170 - Security best practice indicator 61

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.71. OSVM-171 - Security best practice indicator 62

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.72. OSVM-172 - Security best practice indicator 63

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.73. OSVM-173 - Security best practice indicator 64

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.74. OSVM-174 - Security best practice indicator 65

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.75. OSVM-175 - Security best practice indicator 66

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.76. OSVM-176 - Security best practice indicator 67

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.77. OSVM-177 - Security best practice indicator 68

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.78. OSVM-178 - Security best practice indicator 69

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.79. OSVM-179 - Security best practice indicator 70

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.80. OSVM-180 - Security best practice indicator 71

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.81. OSVM-181 - Security best practice indicator 72

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.82. OSVM-182 - Security best practice indicator 73

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.83. OSVM-183 - Security best practice indicator 74

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.84. OSVM-184 - Security best practice indicator 75

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.85. OSVM-185 - Security best practice indicator 76

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.86. OSVM-186 - Security best practice indicator 77

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.87. OSVM-187 - Security best practice indicator 78

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.88. OSVM-188 - Security best practice indicator 79

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.89. OSVM-189 - Security best practice indicator 80

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.90. OSVM-190 - Security best practice indicator 81

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.91. OSVM-191 - Security best practice indicator 82

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.92. OSVM-192 - Security best practice indicator 83

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.93. OSVM-193 - Security best practice indicator 84

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.94. OSVM-194 - Security best practice indicator 85

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.95. OSVM-195 - Security best practice indicator 86

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.96. OSVM-196 - Security best practice indicator 87

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.97. OSVM-197 - Security best practice indicator 88

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.98. OSVM-198 - Security best practice indicator 89

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.99. OSVM-199 - Security best practice indicator 90

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.100. OSVM-200 - Security best practice indicator 91

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.101. OSVM-201 - Security best practice indicator 92

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.102. OSVM-202 - Security best practice indicator 93

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.103. OSVM-203 - Security best practice indicator 94

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.104. OSVM-204 - Security best practice indicator 95

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.105. OSVM-205 - Security best practice indicator 96

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.106. OSVM-206 - Security best practice indicator 97

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.107. OSVM-207 - Security best practice indicator 98

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.108. OSVM-208 - Security best practice indicator 99

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.109. OSVM-209 - Security best practice indicator 100

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.110. OSVM-210 - Security best practice indicator 101

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.111. OSVM-211 - Security best practice indicator 102

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.112. OSVM-212 - Security best practice indicator 103

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.113. OSVM-213 - Security best practice indicator 104

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.114. OSVM-214 - Security best practice indicator 105

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.115. OSVM-215 - Security best practice indicator 106

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.116. OSVM-216 - Security best practice indicator 107

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.117. OSVM-217 - Security best practice indicator 108

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.118. OSVM-218 - Security best practice indicator 109

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.119. OSVM-219 - Security best practice indicator 110

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.120. OSVM-220 - Security best practice indicator 111

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.121. OSVM-221 - Security best practice indicator 112

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.122. OSVM-222 - Security best practice indicator 113

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.123. OSVM-223 - Security best practice indicator 114

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.124. OSVM-224 - Security best practice indicator 115

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.125. OSVM-225 - Security best practice indicator 116

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.126. OSVM-226 - Security best practice indicator 117

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.127. OSVM-227 - Security best practice indicator 118

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.128. OSVM-228 - Security best practice indicator 119

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.129. OSVM-229 - Security best practice indicator 120

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.130. OSVM-230 - Security best practice indicator 121

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.131. OSVM-231 - Security best practice indicator 122

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.132. OSVM-232 - Security best practice indicator 123

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.133. OSVM-233 - Security best practice indicator 124

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.134. OSVM-234 - Security best practice indicator 125

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.135. OSVM-235 - Security best practice indicator 126

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.136. OSVM-236 - Security best practice indicator 127

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.137. OSVM-237 - Security best practice indicator 128

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.138. OSVM-238 - Security best practice indicator 129

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.139. OSVM-239 - Security best practice indicator 130

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.140. OSVM-240 - Security best practice indicator 131

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.141. OSVM-241 - Security best practice indicator 132

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.142. OSVM-242 - Security best practice indicator 133

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.143. OSVM-243 - Security best practice indicator 134

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.144. OSVM-244 - Security best practice indicator 135

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.145. OSVM-245 - Security best practice indicator 136

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.146. OSVM-246 - Security best practice indicator 137

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.147. OSVM-247 - Security best practice indicator 138

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.148. OSVM-248 - Security best practice indicator 139

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.149. OSVM-249 - Security best practice indicator 140

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.150. OSVM-250 - Security best practice indicator 141

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.151. OSVM-251 - Security best practice indicator 142

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.152. OSVM-252 - Security best practice indicator 143

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.153. OSVM-253 - Security best practice indicator 144

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.154. OSVM-254 - Security best practice indicator 145

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.155. OSVM-255 - Security best practice indicator 146

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.156. OSVM-256 - Security best practice indicator 147

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.157. OSVM-257 - Security best practice indicator 148

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.158. OSVM-258 - Security best practice indicator 149

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.159. OSVM-259 - Security best practice indicator 150

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.160. OSVM-260 - Security best practice indicator 151

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.161. OSVM-261 - Security best practice indicator 152

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.162. OSVM-262 - Security best practice indicator 153

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.163. OSVM-263 - Security best practice indicator 154

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.164. OSVM-264 - Security best practice indicator 155

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.165. OSVM-265 - Security best practice indicator 156

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.166. OSVM-266 - Security best practice indicator 157

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.167. OSVM-267 - Security best practice indicator 158

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.168. OSVM-268 - Security best practice indicator 159

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.7.169. OSVM-269 - Security best practice indicator 160

Severity: Info **Category:** Security

Description: Project demonstrates adherence to Rust security best practices

Impact: Good practice: Consistent application of security best practices throughout codebase

Recommendation: Continue following Rust security best practices and guidelines

Code Location: Project-wide

References:

- https://www.rust-lang.org/governance/wgs/wg-secure-code

3.8. Solana Authority Management (3 findings)

3.8.1. OSVM-SOL-1b24a1760f02dd8c - Unsafe authority transfer pattern

Severity: High **Category:** Solana Authority Management **CWE ID:** CWE-269 **CVSS Score:** 8

Description: File agent-registry

Impact: Authority could be transferred to incorrect or malicious addresses

Recommendation: Implement two-step authority transfer with pending/accept pattern and proper validation

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html#authority-transfer
- https://docs.solana.com/developing/programming-model/accounts#ownership

3.8.2. OSVM-SOL-3c3092e93b3afd7f - Unsafe authority transfer pattern

Severity: High **Category:** Solana Authority Management **CWE ID:** CWE-269 **CVSS Score:** 8

Description: File common

Impact: Authority could be transferred to incorrect or malicious addresses

Recommendation: Implement two-step authority transfer with pending/accept pattern and proper validation

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html#authority-transfer
- https://docs.solana.com/developing/programming-model/accounts#ownership

3.8.3. OSVM-SOL-4e3a82de4a2f5576 - Unsafe authority transfer pattern

Severity: High **Category:** Solana Authority Management **CWE ID:** CWE-269 **CVSS Score:** 8

Description: File mcp-server-registry

Impact: Authority could be transferred to incorrect or malicious addresses

Recommendation: Implement two-step authority transfer with pending/accept pattern and proper validation

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html#authority-transfer
- https://docs.solana.com/developing/programming-model/accounts#ownership

3.9. Solana CPI Safety (3 findings)

3.9.1. OSVM-SOL-baa91ae8cbee6e39 - Missing account reload after CPI

Severity: High **Category:** Solana CPI Safety **CWE ID:** CWE-362 **CVSS Score:** 7

Description: File agent-registry

Impact: Account data may be stale after CPI, leading to incorrect program behavior and potential race conditions

Recommendation: Always reload account data after CPI operations to ensure data consistency and prevent race conditions. Use account.reload() or fetch fresh account data.

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html#account-reloading
- https://docs.solana.com/developing/programming-model/calling-between-programs#reentrancy

3.9.2. OSVM-SOL-1d674f37e203f4cd - Missing account reload after CPI

Severity: High **Category:** Solana CPI Safety **CWE ID:** CWE-362 **CVSS Score:** 7

Description: File common

Impact: Account data may be stale after CPI, leading to incorrect program behavior and potential race conditions

Recommendation: Always reload account data after CPI operations to ensure data consistency and prevent race conditions. Use account.reload() or fetch fresh account data.

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html#account-reloading
- https://docs.solana.com/developing/programming-model/calling-between-programs#reentrancy

3.9.3. OSVM-SOL-4f402148be2ee2a6 - Missing account reload after CPI

Severity: High **Category:** Solana CPI Safety **CWE ID:** CWE-362 **CVSS Score:** 7

Description: File mcp-server-registry

Impact: Account data may be stale after CPI, leading to incorrect program behavior and potential race conditions

Recommendation: Always reload account data after CPI operations to ensure data consistency and prevent race conditions. Use account.reload() or fetch fresh account data.

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html#account-reloading
- https://docs.solana.com/developing/programming-model/calling-between-programs#reentrancy

3.10. Solana Security (425 findings)

3.10.1. OSVM-SOL-2f7ac908aaeb13e2 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File svmai-token

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: svmai-token:svmai-token

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.2. OSVM-SOL-76c541275e001dcf - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File svmai-token

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: svmai-token:svmai-token

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.3. OSVM-SOL-7bc2c514d1420dde - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.4. OSVM-SOL-49da4b2599e80d8f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.5. OSVM-SOL-32ae498cb1d33338 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.6. OSVM-SOL-16c9f58e74da76db - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.7. OSVM-SOL-17dd6d9359c8b0bc - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.8. OSVM-SOL-89ac3360dc2ca6a1 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.9. OSVM-SOL-6743df762d56a567 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.10. OSVM-SOL-639c52f2f8e99ce2 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.11. OSVM-SOL-7bcd4f88a954f684 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.12. OSVM-SOL-1f82f0253acccf74 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.13. OSVM-SOL-aa8be72b650b42ee - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.14. OSVM-SOL-78d9cf5927fadddc - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.15. OSVM-SOL-a065a028ad45d2ad - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.16. OSVM-SOL-d8c0c18f5647367b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.17. OSVM-SOL-aacb03d47bfbc5c9 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.18. OSVM-SOL-53f14763693350d9 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.19. OSVM-SOL-642d44312c6ea809 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.20. OSVM-SOL-8da576035ba6f3fb - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.21. OSVM-SOL-689c696d937e0e27 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.22. OSVM-SOL-8eec240b1f5ce115 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.23. OSVM-SOL-1f7d1802d25c5018 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.24. OSVM-SOL-79a58c8f5f89f2d5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.25. OSVM-SOL-bb1aa2c02735195a - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.26. OSVM-SOL-f3eabe58cd24c556 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.27. OSVM-SOL-2373896216129d63 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.28. OSVM-SOL-833d34106cbac412 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.29. OSVM-SOL-42caf88b0bfe7ce0 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.30. OSVM-SOL-420abd04f2482034 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.31. OSVM-SOL-5f3500a66f830840 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.32. OSVM-SOL-334689a607b36006 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.33. OSVM-SOL-551cc1245fa9d84e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.34. OSVM-SOL-8f0b20ab873d5fe8 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.35. OSVM-SOL-bc4b2768c10b0bc8 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.36. OSVM-SOL-07cc4b278d1f2c04 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.37. OSVM-SOL-1a701286b9b899ca - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.38. OSVM-SOL-41a0670a50affcb2 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.39. OSVM-SOL-8664670e6712e9d1 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.40. OSVM-SOL-9b67b9441046e658 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.41. OSVM-SOL-2935b7af67c03caf - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.42. OSVM-SOL-a1db5e15cc59af1d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.43. OSVM-SOL-4128885a19c014b2 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.44. OSVM-SOL-b26209deac768d97 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.45. OSVM-SOL-d45e6e412e3e5aae - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.46. OSVM-SOL-356141a803d081c8 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.47. OSVM-SOL-ec134470b093447f - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.48. OSVM-SOL-588d3c651f07874f - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.49. OSVM-SOL-72002b00a3a274c6 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.50. OSVM-SOL-665522f94376fef7 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.51. OSVM-SOL-493f0f13cf5ec371 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.52. OSVM-SOL-ec8fa764e12aa6b7 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.53. OSVM-SOL-4506442963da3bc1 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.54. OSVM-SOL-a1c84e5fe73b0db3 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.55. OSVM-SOL-36d577538bf101a4 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.56. OSVM-SOL-7ef857d73dcc3f15 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.57. OSVM-SOL-db79f50de66d9447 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.58. OSVM-SOL-aa265d5105da8e0f - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.59. OSVM-SOL-70e7a25a6462ea40 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.60. OSVM-SOL-47a1ebaf85f69627 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.61. OSVM-SOL-b75ff2073099f970 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.62. OSVM-SOL-ca3ca7590a7b6c2f - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.63. OSVM-SOL-063084e196136fce - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.64. OSVM-SOL-95802422e59c2d8f - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.65. OSVM-SOL-6f3c9bc867c3519d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.66. OSVM-SOL-a30d9a56df7eed60 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.67. OSVM-SOL-3afb2602aab4105c - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.68. OSVM-SOL-13976798755512fa - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.69. OSVM-SOL-4524b1830b076574 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.70. OSVM-SOL-93a86b29e0ce4e9e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.71. OSVM-SOL-763c3e75ad33d70f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.72. OSVM-SOL-1e013898c32a0a0b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.73. OSVM-SOL-10350848c4962e72 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.74. OSVM-SOL-49133182c90f3626 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.75. OSVM-SOL-027557caa24868e3 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.76. OSVM-SOL-1c8917f40e720bb3 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.77. OSVM-SOL-4abf77e001e8c0ab - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.78. OSVM-SOL-357232e5357f76a3 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.79. OSVM-SOL-c5a07764f7b76310 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.80. OSVM-SOL-6490e04093dd6c39 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts

- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.81. OSVM-SOL-098087d1b663ae39 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.82. OSVM-SOL-46069e36d5a41a30 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.83. OSVM-SOL-658321703dba23e0 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.84. OSVM-SOL-391562de6188a66a - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.85. OSVM-SOL-b0e82040805369e4 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.86. OSVM-SOL-343c161de3a1faef - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.87. OSVM-SOL-e8b6d416481d9b28 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.88. OSVM-SOL-1d3f1fc5b4d95034 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File agent-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.89. OSVM-SOL-e7570ef3da59c171 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.90. OSVM-SOL-90bdf68968ac7d68 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.91. OSVM-SOL-c9d9a96c8d34ef17 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.92. OSVM-SOL-fc8cf856a2b82149 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.93. OSVM-SOL-74f737a3b9e92dec - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.94. OSVM-SOL-f7bb57cdb8eaefa5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.95. OSVM-SOL-e6ff02981e70fb24 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.96. OSVM-SOL-37fc8b89d2f4de65 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.97. OSVM-SOL-e6aac7a63286554c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.98. OSVM-SOL-7583b2f4fc4baefd - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.99. OSVM-SOL-4c32b7ff1cc7675b - Missing program ID validation before CPI

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-20 **CVSS Score:** 9

Description: File agent-registry

Impact: Arbitrary program execution vulnerability - attacker can invoke malicious programs

Recommendation: Always validate the program ID before making cross-program invocations

Code Location: agent-registry:agent-registry

References:

- https://docs.solana.com/developing/programming-model/calling-between-programs
- https://github.com/coral-xyz/sealevel-attacks/tree/master/programs/0-arbitrary-cpi

3.10.100. OSVM-SOL-0d13bdea9d2dc300 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.101. OSVM-SOL-b8e13d117906c336 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.102. OSVM-SOL-2134ef7829958ae3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.103. OSVM-SOL-0764b265acfe0544 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.104. OSVM-SOL-4130b8b5e3c536fe - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.105. OSVM-SOL-4fc43067135bf8d2 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.106. OSVM-SOL-ad073f7b0aae5131 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.107. OSVM-SOL-e4b72c9d692c55e9 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.108. OSVM-SOL-ede1a4bea4630e1a - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.109. OSVM-SOL-8e6d78ee2928c05d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.110. OSVM-SOL-610bf4e746071fc9 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.111. OSVM-SOL-017938b82fe3bc6f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.112. OSVM-SOL-e9e067d90d8bb46d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.113. OSVM-SOL-017103b88fb8af5d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.114. OSVM-SOL-29cd23ccb0b619b3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.115. OSVM-SOL-4553df74c2896e78 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.116. OSVM-SOL-1664b00ee61becaa - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.117. OSVM-SOL-46a2cc8b418cb9b5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.118. OSVM-SOL-748baee68b8d469a - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.119. OSVM-SOL-4fc049287662fbd3 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.120. OSVM-SOL-885d68a8ac60c49f - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.121. OSVM-SOL-a7a9dffae51ee5d6 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.122. OSVM-SOL-dc0703c6c076a3e6 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.123. OSVM-SOL-f0898e118de935ad - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.124. OSVM-SOL-d34690706f60f332 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.125. OSVM-SOL-2a5e0c0e683309fc - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.126. OSVM-SOL-c9d741fd4cae86fc - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.127. OSVM-SOL-97767abe92b7495b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.128. OSVM-SOL-8c17a58ee5213ad5 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.129. OSVM-SOL-2801b72c83e43739 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.130. OSVM-SOL-fc33c4a2f4f88f7b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.131. OSVM-SOL-479927bed0696888 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.132. OSVM-SOL-d361076facab0dd8 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.133. OSVM-SOL-c31fec2719cd9e3c - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.134. OSVM-SOL-590cb6a449f62be3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.135. OSVM-SOL-4a29650e23dc70ab - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.136. OSVM-SOL-7dd94720c0700b88 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.137. OSVM-SOL-615d5b45e5afb6de - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.138. OSVM-SOL-524f8fb8a8e01832 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.139. OSVM-SOL-1e3f501565ec1e80 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.140. OSVM-SOL-baf0757fe695dd06 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.141. OSVM-SOL-b3b9073f08c79e13 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.142. OSVM-SOL-f28bc49df33d0447 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.143. OSVM-SOL-46770d2d96fa6725 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.144. OSVM-SOL-16d5124716d299ad - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.145. OSVM-SOL-6364ee1e3b005970 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.146. OSVM-SOL-2638624ff3c58b48 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.147. OSVM-SOL-fe1557402947db61 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.148. OSVM-SOL-3556eef08fc3a4b4 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.149. OSVM-SOL-cf492bd197f129e4 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.150. OSVM-SOL-768109cfbef79e8b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.151. OSVM-SOL-8a2ac73f2bbf366f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.152. OSVM-SOL-eae921232c2aa76b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.153. OSVM-SOL-f4da45a790d4e47d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.154. OSVM-SOL-a5113791da04ff8d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.155. OSVM-SOL-342b348f9bfec9db - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.156. OSVM-SOL-277699ccb2e7ecd3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.157. OSVM-SOL-d934df1b4e17023c - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.158. OSVM-SOL-619817c6bdd61dab - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.159. OSVM-SOL-c9694fd720f90902 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.160. OSVM-SOL-dba82441e36b136b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.161. OSVM-SOL-ec978bee64f0c2f5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.162. OSVM-SOL-5d7240a7bc3968e4 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.163. OSVM-SOL-64ccf44421165040 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.164. OSVM-SOL-9e7d0b7e42ae58f5 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.165. OSVM-SOL-5a9344aae4944005 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.166. OSVM-SOL-a1b5e72442cef8ef - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.167. OSVM-SOL-f01260cdfda8999e - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.168. OSVM-SOL-28d7e7762992d89f - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.169. OSVM-SOL-20d74eabb497990f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.170. OSVM-SOL-0dc6520b10383f03 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.171. OSVM-SOL-2e220c6600d9556e - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.172. OSVM-SOL-2c10584bd9ef60c4 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.173. OSVM-SOL-e503998d307ce433 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.174. OSVM-SOL-38804d4e940cf4ed - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.175. OSVM-SOL-055e192f9d8d3867 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.176. OSVM-SOL-2d63ca904b15564e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.177. OSVM-SOL-e4b0738ce9d57818 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.178. OSVM-SOL-a5f28de3bb296492 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.179. OSVM-SOL-df0febacf901d158 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.180. OSVM-SOL-68babcb46860dbe4 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.181. OSVM-SOL-50ea89eea990c3ea - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.182. OSVM-SOL-496bb96fbfd4f3d3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.183. OSVM-SOL-8975f8d76a9afc91 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.184. OSVM-SOL-a316748fc2783692 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.185. OSVM-SOL-fe5f583df2cc0180 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.186. OSVM-SOL-43c0df9fce8a7d8b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.187. OSVM-SOL-15db6fb93a757627 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.188. OSVM-SOL-a13a347c49e8fd9c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.189. OSVM-SOL-1e9ad8e3a8a8a1ec - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.190. OSVM-SOL-ab09e3c8f167ba58 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.191. OSVM-SOL-1d9b1a4d046d8f4f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.192. OSVM-SOL-843c987f572c9713 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.193. OSVM-SOL-d1e871243a822bdf - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.194. OSVM-SOL-c4c83768d69a422b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.195. OSVM-SOL-61df24ddf52a9ca0 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.196. OSVM-SOL-eab1f70c59fcfce1 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.197. OSVM-SOL-3467e853dc58f6d4 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.198. OSVM-SOL-5fe6187ddd1bff0d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.199. OSVM-SOL-42b7c4ae2287996d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.200. OSVM-SOL-4a40761bc91062f1 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.201. OSVM-SOL-7e707ee55e316993 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.202. OSVM-SOL-e33041903f0ea655 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File agent-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.203. OSVM-SOL-219f786aa780ccdd - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File agent-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: agent-registry:agent-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.204. OSVM-SOL-791a561280783645 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.205. OSVM-SOL-8c7b661d8fe8da05 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File common

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.206. OSVM-SOL-833e817b9e9bfd5f - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File common

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: common:common

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.207. OSVM-SOL-16e28db58bb0b8d4 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File common

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: common:common

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.208. OSVM-SOL-523d6416e2c8072e - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File common

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: common:common

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.209. OSVM-SOL-5e7b136b366ebc27 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File common

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: common:common

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.210. OSVM-SOL-8f7796fa77eff17d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.211. OSVM-SOL-c22c4c1cc61bbd25 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.212. OSVM-SOL-3eccb73da18a5fd3 - Missing program ID validation before CPI

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-20 **CVSS Score:** 9

Description: File common

Impact: Arbitrary program execution vulnerability - attacker can invoke malicious programs

Recommendation: Always validate the program ID before making cross-program invocations

Code Location: common:common

References:

- https://docs.solana.com/developing/programming-model/calling-between-programs
- https://github.com/coral-xyz/sealevel-attacks/tree/master/programs/0-arbitrary-cpi

3.10.213. OSVM-SOL-610e3de74ebcfc7b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.214. OSVM-SOL-e3117b6641fd7e1e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html

- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.215. OSVM-SOL-dd5640000455d66e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.216. OSVM-SOL-d169344eefb95c34 - Missing program ID validation before CPI

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-20 **CVSS Score:** 9

Description: File common

Impact: Arbitrary program execution vulnerability - attacker can invoke malicious programs

Recommendation: Always validate the program ID before making cross-program invocations

Code Location: common:common

References:

- https://docs.solana.com/developing/programming-model/calling-between-programs
- https://github.com/coral-xyz/sealevel-attacks/tree/master/programs/0-arbitrary-cpi

3.10.217. OSVM-SOL-f417aab29751d983 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File common

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: common:common

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.218. OSVM-SOL-ac2d88244fb20235 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.219. OSVM-SOL-f34e38c25668bd44 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.220. OSVM-SOL-8154517d4751f8b0 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.221. OSVM-SOL-dd5cd8cf308b0b18 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.222. OSVM-SOL-a37e9031fd81bb8d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.223. OSVM-SOL-42654f17ea9ef915 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.224. OSVM-SOL-75d29924c4a52e0d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.225. OSVM-SOL-3344d1e0cb939135 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.226. OSVM-SOL-ffd0a6263f49bf8a - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.227. OSVM-SOL-638a16375b839cd5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.228. OSVM-SOL-afc724e043c08a07 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.229. OSVM-SOL-be4ce20a69bca703 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.230. OSVM-SOL-699a4e4ed5e49ab3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.231. OSVM-SOL-40f548f963ec8fe9 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.232. OSVM-SOL-443f55c767952240 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.233. OSVM-SOL-6adaa8c470d0c90d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.234. OSVM-SOL-8745ca7a739994d3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.235. OSVM-SOL-f49a5d9326a038f1 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.236. OSVM-SOL-70e12f61490dd17b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.237. OSVM-SOL-2602fbd25bb86bd4 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.238. OSVM-SOL-e80cb96865bfd722 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.239. OSVM-SOL-b2f87867aced1685 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.240. OSVM-SOL-45f8a92c18ae9f23 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.241. OSVM-SOL-ddc095050ada3f16 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.242. OSVM-SOL-5e220c566096828b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.243. OSVM-SOL-08ccc984b25520dc - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.244. OSVM-SOL-0e256e95305d18a7 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.245. OSVM-SOL-cb502c661ddfd352 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.246. OSVM-SOL-c433b5066a840d8e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.247. OSVM-SOL-7b00d4215a36b55d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.248. OSVM-SOL-bab0a7f4890a3cb8 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.249. OSVM-SOL-24c7a158d4893aba - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.250. OSVM-SOL-59188c7d62c8338c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.251. OSVM-SOL-e4334b7a8fcca716 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.252. OSVM-SOL-382e91ce380f7383 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.253. OSVM-SOL-be6494621c17e7b5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.254. OSVM-SOL-fa91f756c957abb1 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.255. OSVM-SOL-58fcb16b40dc28a9 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.256. OSVM-SOL-ea864ee99f6df4d9 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.257. OSVM-SOL-78b764a6be9dc2f6 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.258. OSVM-SOL-869cae6502d7cd2c - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.259. OSVM-SOL-06dceb4b24aad0d4 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.260. OSVM-SOL-88ab246a23c018a8 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.261. OSVM-SOL-ee480d0f3ff2cf97 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.262. OSVM-SOL-bd8c459b0e7689a2 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.263. OSVM-SOL-2c8b13064c6dff58 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.264. OSVM-SOL-bec90bb9a3f1b03c - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.265. OSVM-SOL-eaa28fa9ddd956e8 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts

- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.266. OSVM-SOL-357c4ea8ee34326b - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.267. OSVM-SOL-0e861ad926496733 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.268. OSVM-SOL-5c9b61db91969b47 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.269. OSVM-SOL-5114684c00afc9e9 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.270. OSVM-SOL-a4b4c5637499d244 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.271. OSVM-SOL-d3690db02003d6fa - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.272. OSVM-SOL-b12c241f1a47a56f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.273. OSVM-SOL-20acdde7571577c1 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.274. OSVM-SOL-c0fb841a32aa200e - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.275. OSVM-SOL-76f8767dca453a10 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.276. OSVM-SOL-8528debad8557073 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.277. OSVM-SOL-30e432d9b25760b9 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.278. OSVM-SOL-8663c08c78119ddf - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.279. OSVM-SOL-7785019cc74e8beb - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.280. OSVM-SOL-c82d3c38396ad78f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.281. OSVM-SOL-b980ad69d4024a75 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.282. OSVM-SOL-f099ae478cea84b5 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.283. OSVM-SOL-f4bdd9c37a760950 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.284. OSVM-SOL-f4955f0ab22d6cba - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.285. OSVM-SOL-859bec4f843583e5 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.286. OSVM-SOL-0c14d37e61bb570e - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.287. OSVM-SOL-f79b616259c10c28 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File mcp-server-registry

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.288. OSVM-SOL-9ea110e3462bb7dc - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.289. OSVM-SOL-8d7a6cdbca1a8ef4 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.290. OSVM-SOL-556c2da980bcf918 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.291. OSVM-SOL-d9bcaefc64c9096d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.292. OSVM-SOL-2b90d13fc9b15b63 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.293. OSVM-SOL-fbdb9d01a687df5f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.294. OSVM-SOL-3eeeb19028813428 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.295. OSVM-SOL-3f00d7d167e067a2 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.296. OSVM-SOL-02056ff9287fbf45 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.297. OSVM-SOL-411baac8d444cdcc - Missing program ID validation before CPI

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-20 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Arbitrary program execution vulnerability - attacker can invoke malicious programs

Recommendation: Always validate the program ID before making cross-program invocations

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://docs.solana.com/developing/programming-model/calling-between-programs
- https://github.com/coral-xyz/sealevel-attacks/tree/master/programs/0-arbitrary-cpi

3.10.298. OSVM-SOL-1d20612bdcb99b67 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.299. OSVM-SOL-d6e1a24c3699a2c5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.300. OSVM-SOL-93465d7cf1814744 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.301. OSVM-SOL-7d56b681d372ff12 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.302. OSVM-SOL-3d171625c0a37a19 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.303. OSVM-SOL-e26eaaa1d04bd390 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.304. OSVM-SOL-a32962eab570ccb4 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.305. OSVM-SOL-acc143092deb8f59 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.306. OSVM-SOL-4b9c2f7881c9da1d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.307. OSVM-SOL-89f9f269f2cbcdde - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.308. OSVM-SOL-b101777518e10112 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.309. OSVM-SOL-31e103bae415d1b3 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.310. OSVM-SOL-8ee5af0fd9ba6f06 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.311. OSVM-SOL-f9d291d72bf19014 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.312. OSVM-SOL-0c801277898525ea - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.313. OSVM-SOL-1155c6cbae4f8dba - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.314. OSVM-SOL-d006d2f606c5f62c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.315. OSVM-SOL-63cb9440f1d38efe - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.316. OSVM-SOL-404f34bf12f0f2c9 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.317. OSVM-SOL-191cec08faa67c37 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.318. OSVM-SOL-27ea2093a4bf337e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.319. OSVM-SOL-f37e88742e8289c2 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.320. OSVM-SOL-28fe318d8b6247fc - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.321. OSVM-SOL-fd978e1a54222fc9 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.322. OSVM-SOL-d1e4e98365c680b5 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.323. OSVM-SOL-e9451e1416a5211c - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.324. OSVM-SOL-0954f26d75d8afd8 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.325. OSVM-SOL-9d190e81a235dc50 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.326. OSVM-SOL-f4957f9b21ad9438 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.327. OSVM-SOL-49dc4a2fda923624 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.328. OSVM-SOL-361d441eb1301a24 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.329. OSVM-SOL-c90944debcc08c03 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.330. OSVM-SOL-e478cabeff826e92 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.331. OSVM-SOL-fdea6c98ce5c820e - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.332. OSVM-SOL-a16b006035a333ef - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.333. OSVM-SOL-651919df87d9ea58 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.334. OSVM-SOL-3a9ed4d458ccdb69 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.335. OSVM-SOL-5c9f7b8f41fa7d50 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.336. OSVM-SOL-5c1f67c1136ad179 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.337. OSVM-SOL-7815734ef49b6c86 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.338. OSVM-SOL-8b209de38e28a6b4 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.339. OSVM-SOL-603db313ef84df24 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.340. OSVM-SOL-0706236473466bcf - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.341. OSVM-SOL-7ae33946faa4da4b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.342. OSVM-SOL-ff99825fbd3d82a7 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.343. OSVM-SOL-75339a71ce999a62 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.344. OSVM-SOL-1a09fa32b3feadb7 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.345. OSVM-SOL-01357df30f003c3b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.346. OSVM-SOL-5f439f22500321fb - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.347. OSVM-SOL-1757683918165115 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.348. OSVM-SOL-b7ca4fa4d99ee2da - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.349. OSVM-SOL-ee93d7afd12344c2 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.350. OSVM-SOL-7555804314cafcd3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.351. OSVM-SOL-69cdc57b20045a2b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.352. OSVM-SOL-3003c50a173cd557 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.353. OSVM-SOL-514ec6039bf89440 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.354. OSVM-SOL-245861f6d166412e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.355. OSVM-SOL-11fa3430f2e1a1fe - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.356. OSVM-SOL-6e5a58de7cf638b3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.357. OSVM-SOL-84a50d65c64df9b3 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.358. OSVM-SOL-9cb7df80fa0468d5 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.359. OSVM-SOL-56ec7b15a8bda141 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.360. OSVM-SOL-ae464520bf23bff2 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.361. OSVM-SOL-480dda0c6a8f3e2f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.362. OSVM-SOL-c42bbaa92595a09b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.363. OSVM-SOL-ca594c01d7d92177 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.364. OSVM-SOL-69c92ef495e9e4a8 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.365. OSVM-SOL-06e25599d9f8ec32 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.366. OSVM-SOL-de4eb763270f12cf - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.367. OSVM-SOL-889a3be074a9fb98 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.368. OSVM-SOL-6809c1d1ba753f9d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.369. OSVM-SOL-4fec949689db6308 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.370. OSVM-SOL-fc5c0f7f17ebfb5c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.371. OSVM-SOL-fa1722f47b1d37d1 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.372. OSVM-SOL-df7ec69051e60269 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.373. OSVM-SOL-5d0b2e04dd16def9 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.374. OSVM-SOL-5fad3fc32c13c92c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.375. OSVM-SOL-0e03ad7d7e1f64f7 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.376. OSVM-SOL-f80c7d72849af870 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.377. OSVM-SOL-6144d3b8830343f5 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.378. OSVM-SOL-bcc1861e26d40d96 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.379. OSVM-SOL-304b22a41a44ec6e - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.380. OSVM-SOL-d650478369f90d92 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.381. OSVM-SOL-c80264b8ea456fad - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.382. OSVM-SOL-dff50c374db18fcc - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.383. OSVM-SOL-c33cd3291a4575c6 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.384. OSVM-SOL-f89fbaee2575ce6b - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.385. OSVM-SOL-75fa260f6e49bc34 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.386. OSVM-SOL-4677f2f0e52f1b83 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.387. OSVM-SOL-33d6df0858540dae - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.388. OSVM-SOL-2660656bda6c8000 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.389. OSVM-SOL-2bf2bbb0b5402b25 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.390. OSVM-SOL-61906759ec1270a9 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.391. OSVM-SOL-f9d78369074f68af - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.392. OSVM-SOL-98b612cae43d3a96 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.393. OSVM-SOL-fb6abb7c7d6ba51c - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.394. OSVM-SOL-bbeb172941ce8cce - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File mcp-server-registry

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.395. OSVM-SOL-b2f526a2fec2be69 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File mcp-server-registry

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: mcp-server-registry:mcp-server-registry

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.396. OSVM-SOL-225578720ecfb435 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.397. OSVM-SOL-1fd6bbb23f32618f - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.398. OSVM-SOL-377df4ed68a4edeb - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.399. OSVM-SOL-055a453809dcf99b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.400. OSVM-SOL-e09ac855392f5417 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.401. OSVM-SOL-d30d92613da8f13b - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.402. OSVM-SOL-e362acee68efbf41 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.403. OSVM-SOL-315eaae238f70806 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.404. OSVM-SOL-29d654f19c320eb0 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File rust

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: rust:rust

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.405. OSVM-SOL-fe6195b03ba58d64 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File rust

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: rust:rust

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.406. OSVM-SOL-5b98dfafcc68da72 - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File rust

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: rust:rust

References:

- https://docs.solana.com/developing/programming-model/accounts
- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.407. OSVM-SOL-a7d0a52445a0778f - Potential hardcoded Solana public key

Severity: Medium **Category:** Solana Security **CWE ID:** CWE-798 **CVSS Score:** 5

Description: File rust

Impact: Hardcoded keys reduce flexibility and may expose sensitive information

Recommendation: Use environment variables or configuration for public keys, or use the Pubkey::from_str() function with constants

Code Location: rust:rust

References:

- https://docs.solana.com/developing/programming-model/accounts

- https://docs.rs/solana-sdk/latest/solana_sdk/pubkey/struct.Pubkey.html

3.10.408. OSVM-SOL-6eb27596d82d4dee - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.409. OSVM-SOL-603c998fdebeeb44 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.410. OSVM-SOL-3ea29cce2ea859e3 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.411. OSVM-SOL-fd14734389ab3c7e - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.412. OSVM-SOL-919453954bbf1d1d - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.413. OSVM-SOL-abc90e9273b9ac96 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.414. OSVM-SOL-3c3c48fefbc85dec - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.415. OSVM-SOL-389d1651afa2148d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.416. OSVM-SOL-63245da408b847e7 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.417. OSVM-SOL-b53e616de6a6fa8d - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.418. OSVM-SOL-959353fa556b2a06 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.419. OSVM-SOL-9bd749884d6e636c - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.420. OSVM-SOL-8afaea1284f140c6 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.421. OSVM-SOL-f2b4cf7d9001ee70 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.422. OSVM-SOL-6452e4eeef6afdc1 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.423. OSVM-SOL-4bcc86cd860f12e7 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

3.10.424. OSVM-SOL-a82cafc3eb1062a7 - Missing account owner validation

Severity: High **Category:** Solana Security **CWE ID:** CWE-284 **CVSS Score:** 7.5

Description: File rust

Impact: Programs could operate on accounts owned by malicious programs

Recommendation: Always verify account ownership before performing operations: account.owner == expected_program_id

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html

3.10.425. OSVM-SOL-664c4cf6a9a6f551 - Missing signer validation in Solana operation

Severity: Critical **Category:** Solana Security **CWE ID:** CWE-862 **CVSS Score:** 9

Description: File rust

Impact: Unauthorized users could execute privileged operations

Recommendation: Always validate that required accounts are signers using is_signer checks

Code Location: rust:rust

References:

- https://book.anchor-lang.com/anchor_bts/security.html
- https://solana-labs.github.io/solana-program-library/anchor/lang/macro.Program.html

4. Security Recommendations

1. Implement regular security audits and penetration testing
2. Keep all dependencies up to date and monitor for security advisories
3. Use proper secret management and avoid hardcoding sensitive information
4. Implement comprehensive logging and monitoring
5. Follow the principle of least privilege for all system components

5. Compliance Notes

- This audit report follows industry security standards and best practices
- Findings are categorized using the Common Weakness Enumeration (CWE) framework
- CVSS scores are provided where applicable to help prioritize remediation efforts
- Critical vulnerabilities require immediate attention and remediation
- Regular security assessments are recommended to maintain security posture

6. Statistics

Metric	Value
Total Findings	793
Findings with CWE	622
Findings with CVSS	793
Findings with Location	790
Unique Categories	10
Average CVSS Score	6.1
Coverage Percentage	99.6%

7. Conclusion

This security audit provides a comprehensive assessment of the OSVM CLI application's security posture. All identified findings should be addressed according to their severity level, with critical and high-severity issues taking priority.

⚠️ **CRITICAL: 197 critical findings require immediate remediation.**

⚠️ **HIGH: 344 high-severity findings should be addressed promptly.**

Regular security assessments and continuous monitoring are recommended to maintain a strong security stance.

Generated by OSVM Security Audit System

End of Report