

Report di Sicurezza – Arbitrum-One – 0x912CE59144191C1204E64559FE8253a0e49E6548

Data: 2025-09-13 20:52 UTC • RPC: arb1.arbitrum.io

Executive Summary

Classificazione complessiva: **CRITICAL.**

- Proxy EIP-1967 (slot implementation/admin impostati).
- Opcode DELEGATECALL presente → possibili rischi di delega.
- Opcode SELFDESTRUCT presente → rischio distruzione contratto.
- Superficie di upgrade rilevata (proxy/upgradeTo).

Dettagli (grezzi)

| Chiave | Valore |
|-----------------------------|--|
| bytecode_size | 2593 |
| is_minimal_proxy_eip1167 | False |
| eip1967_proxy | True |
| eip1967.implementation_slot | 000000000000000000000000c4ed0a9ea70d5bcc69f748547650d32cc219d882 |
| eip1967.admin_slot | 000000000000000000000000db216562328215e010f819b5abe947bad4ca961e |
| owner() | 000000000000000000000000cf57572261c7c2bcf21ffd220ea7d1a27d40a827 |
| implementation() | None |
| admin() | None |
| paused() | None |
| has_delegatecall | True |
| has_selfdestruct | True |
| has_sstore | True |
| has_callcode | True |
| upgrade_surface | True |

Raccomandazioni

- Verificare admin multisig; limitare l'upgrade path (UUPS/Transparent).
- Confinare DELEGATECALL ad implementazioni fidate; allowlist e pause-guard.
- Rimuovere/disabilitare SELFDESTRUCT o isolarlo con timelock/owner.

Nota: Controlli euristici via RPC; non sostituiscono un audit completo.