

Report di Sicurezza – Ethereum-Mainnet – 0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2

Data: 2025-09-13 20:52 UTC • RPC: mainnet.infura.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	3124
is_minimal_proxy_eip1167	False
eip1967_proxy	True
eip1967.implementation_slot	00
eip1967.admin_slot	00
owner()	
implementation()	
admin()	
paused()	
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.