

Report di Sicurezza – Ethereum-Mainnet – 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48

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	2186
is_minimal_proxy_eip1167	False
eip1967_proxy	True
eip1967.implementation_slot	00
eip1967.admin_slot	00
owner()	00fcb19e6a322b27c06842a71e8c725399f049ae3a
implementation()	None
admin()	None
paused()	00
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.