DeFi-Yield-Y — Security Audit (Public Summary)

Дата аудита: 2026-06-07 Аудиторы: Краткое резюме

Объект: DeFi-Yield-Y (Yield Farming / Staking, 4 контракта, ~1200 строк).
Результат: Критические и большинство высоких уязвимостей исправлены; есть принятый опер
требует немедленного митигейшена.
Тесты: unit coverage 92%, integration tests on mainnet fork, fuzz 10k cases.

Ключевые находки и статус

Critical — Reentrancy in withdraw() — Исправлено (ReentrancyGuard + checks-effects-inte
after>)
High — Oracle price manipulation via AMM — Исправлено (Chainlink + TWAP window=30min, pr
High — Centralization: emergencyWithdrawAll controlled by single EOA —
Accepted by team; требует миграции в MultiSig + Timelock с дедлайном.
Medium/Low — Upgradeability, events, monitoring — Частично исправлено/рекомендовано.

Рекомендации (важнейшее)

Немедленно перенести контроль экстренных функций в Gnosis Safe multisig(3/5) и внедрить
Внедрить circuit breakers, мониторинг и bug bounty.

Контакты

Для полного technical report и PoC — смотрите Internal Report
или свяжитесь: .