PRZYKŁADOWY RAPORT

Audyt kontraktu | PRO | RAPORT ANALIZY

WYNIK: najwyższy poziom ustalenia WYSOKI, do weryfikacji — Niechroniona zmiana uprawnień (każdy może zmienić właściciela lub rolę) — funkcja DemonstrationOnly.setOwner.

WYSOKI

Co zrobić teraz: zastosuj proponowaną poprawkę (diff w sekcji najważniejszych ustaleń), skompiluj kontrakt, dodaj test, że konto bez uprawnień nie może wywołać tej funkcji, i uruchom analizę ponownie przed wdrożeniem.

Dane demonstracyjne: własny kontrakt testowy, nigdy niewdrożony w sieci. To skrót raportu Audit Pro — pełny raport zawiera też zakres wykonania, pomiary, źródło danych i identyfikator dokumentu.

NAJWAŻNIEJSZE USTALENIA

WYSOKI / Do sprawdzenia: Kandydat heurystyczny ze źródła: Niechroniona zmiana uprawnień (każdy może zmienić właściciela lub rolę) — funkcja DemonstrationOnly.setOwner

Opis: Sygnał Niechroniona zmiana uprawnień (każdy może zmienić właściciela lub rolę) — funkcja DemonstrationOnly.setOwner (UNPROTECTED-PRIVILEGED-WRITE) z analizy statycznej pliku DemonstrationOnly.sol, wiersze 7-7. To wskazówka do przeglądu; nie potwierdza błędu, osiągalności, powiązania ze wdrożonym bytecode ani exploitu.

Rekomendacja naprawy: ogranicz funkcję kontrolą dostępu (np. modyfikator onlyOwner z Ownable albo dwuetapowe przekazanie własności Ownable2Step lub rola AccessControl), odrzucaj adres zerowy (require(next != address(0))) i dodaj test, że konto bez uprawnień nie może zmienić właściciela ani roli.

Proponowana poprawka — diff do Twojego pliku (skompiluj i przetestuj przed wdrożeniem)

```
--- a/DemonstrationOnly.sol
+++ b/DemonstrationOnly.sol
@@ -5,6 +5,7 @@
  address public owner;
  constructor() { owner = msg.sender; }
  function setOwner(address next) external {
+ require(msg.sender == owner);
  owner = next;
  }
  }
```

Dodano kontrolę wywołującego jako pierwszą instrukcję funkcji, z użyciem istniejącej zmiennej stanu "owner" tego kontraktu. Sprawdź, czy to właściwa rola, skompiluj kod i dodaj test konta bez uprawnień.

PRZYKŁADOWY RAPORT

Audyt kontraktu | PRO | RAPORT ANALIZY

CO SPRAWDZIĆ DALEJ

Do sprawdzenia: Następny krok 1 (analityk lub właściciel kontraktu): Zweryfikuj kandydaturę na dokładnym kodzie, stanie i warunkach wskazanych w dowodach przed uznaniem jej za potwierdzony problem.
Do sprawdzenia: Interakcje zewnętrzne: Sprawdź zapisany zakres i dowody tej kontroli. Nierozstrzygnięty status nie dowodzi problemu ani nie oznacza, że dodatkowe dane na pewno rozstrzygną wynik.

GRANICE TEGO RAPORTU

1. To automatyczna analiza dostarczonego kodu, a nie ręczny audyt ani certyfikat bezpieczeństwa.
2. Nie porównaliśmy kodu z wersją wdrożoną w sieci; jeśli kontrakt jest już wdrożony, porównaj kod przed decyzją.
3. Brak ustaleń w obszarze nie dowodzi, że kod jest bezpieczny — reguły wykrywają znane wzorce błędów.
4. Nie wykonano ataku na kontrakt w sieci i nie liczono skutków finansowych.
5. Pełna lista zapisanych ograniczeń (26) jest w załączniku technicznym pliku TXT i w pliku JSON.

Pełne ustalenia, dowody, pomiary i wiersze zakresu pozostają w prywatnym JSON. TXT zawiera szczegółowy opis.