Liquid Royalty AstraSec Audit Remediation

Summary

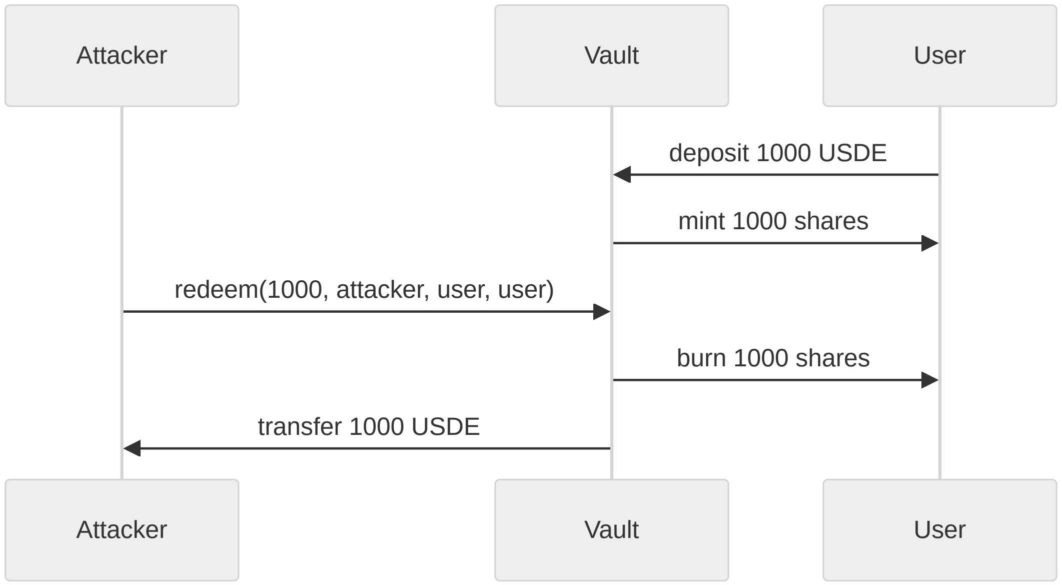
Severity	Fixed
Critical	4
High	4
Medium	4
Low	8

Critical Vulnerabilities

VN001: Missing Allowance Check

Impact: Unauthorized withdrawal of user funds

Issue: `_withdraw()` override missing `_spendAllowance()` check.



Fix:

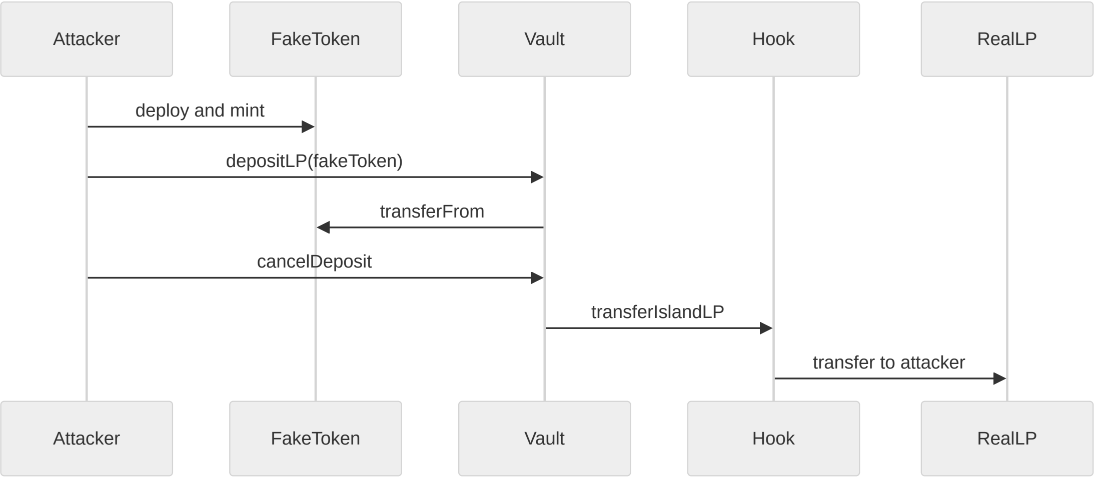
```
if (caller != owner) {
    _spendAllowance(owner, caller, shares);
}
```

Files: `BaseVault.sol`, `ConcreteJuniorVault.sol`

VN002: Unvalidated LP Token

Impact: Exchange fake tokens for real LP tokens

Issue: `depositLP()` accepted any ERC20 address.



Fix:

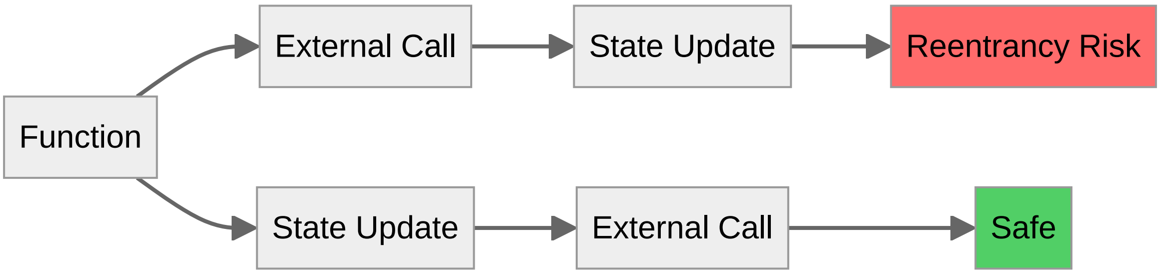
```
if (lpToken != address(kodiakHook.island())) revert InvalidLPToken();
```

Files: `JuniorVault.sol` , `IKodiakVaultHook.sol`

VN003: CEI Pattern Violations

Impact: Reentrancy attack vectors

Issue: State updates after external calls in 6 functions.



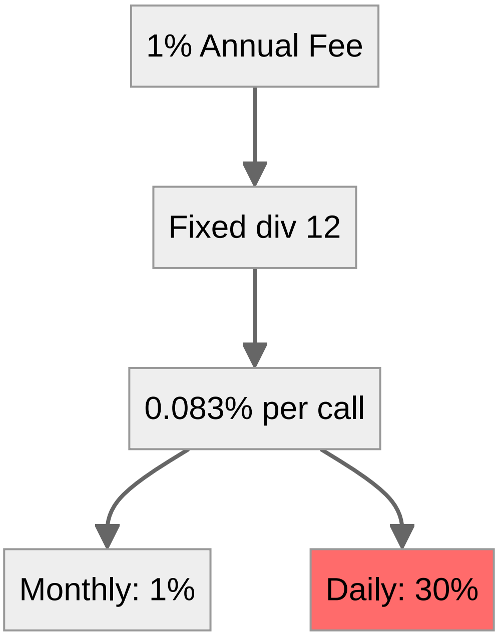
Fix: Moved state updates before external calls.

Files: `ConcreteJuniorVault.sol` , `JuniorVault.sol`

Q3: Time-Based Fee Calculation

Impact: 30× fee overcharging with frequent rebases

Issue: Fee assumed monthly rebases, divided by fixed 12.



Fix:

```
return (vaultValue * MGMT_FEE_ANNUAL * timeElapsed) / (365 days * PRECISION);
```

Files: `FeeLib.sol` , `UnifiedSeniorVault.sol`

Q5: Decimal Handling

Impact: 10 billion× valuation errors for non-18 decimal tokens

Issue: Calculations assumed 18 decimals.

Example:

```
1 WBTC (8 decimals) at $50,000
Expected: 50,000e18 USD
Actual: 5e12 USD
```

Fix:

```
function _normalizeToDecimals(uint256 amount, uint8 from, uint8 to) {
    if (from == to) return amount;
    if (from < to) return amount * 10**(to - from);
    return amount / 10**(from - to);
}
```

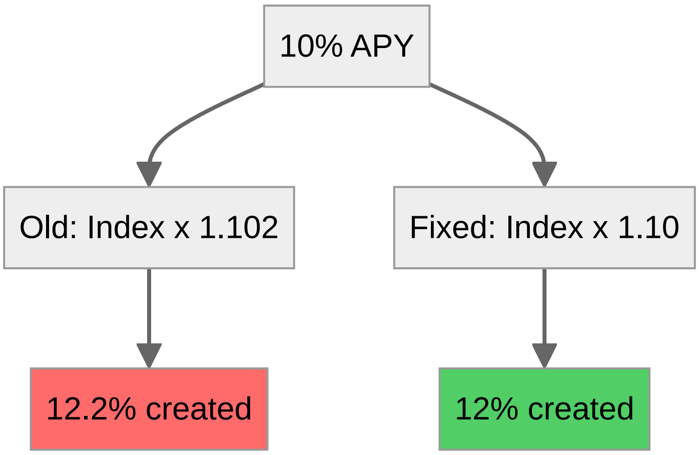
Files: `BaseVault.sol` , `ReserveVault.sol` , `JuniorVault.sol` , `UnifiedSeniorVault.sol`

High Severity

VN001-Audit: Rebase Index Double-Counting

Impact: Phantom token creation

Issue: Performance fee in both index multiplier and minted tokens.



Fix: Removed performance fee from index calculation.

Files: `FeeLib.sol`

VN002-Audit: Backing Ratio Excludes Management Fee

Impact: Incorrect zone detection

Issue: Backing ratio calculated before management fee included.

Fix:

```
uint256 actualNewSupply = selection.newSupply + mgmtFeeTokens;
uint256 finalBackingRatio = _vaultValue / actualNewSupply;
```

Files: `UnifiedSeniorVault.sol`

Medium Severity

N2: Dangerous seedProvider Parameter

Issue: Seeder could pull tokens from any approved user.

Fix: Use `msg.sender` only.

N4: No Minimum Fee Schedule

Issue: Admin could set 1 second interval.

Fix: Require minimum 30 days.

N10: Stale Slippage Protection

Issue: Same-block deposits invalidate `minLPTokens` .

Fix: Added `expectedIdle` and `maxDeviation` parameters.

Low Severity

N1-2: Share Calculation

Replaced manual calculation with `previewDeposit()`.

N3: Duplicate Logic

Refactored array removal into helpers.

N5: ERC20 Compatibility

Replaced 8 `transfer()` with `safeTransfer()`.

N7: Rounding Direction

Changed `_burn()` from floor to ceiling.

N9: Redundant Functions

Removed `setSeniorVault()`, `setJuniorReserve()`.

N10-Router: Dead Code

Removed unused `_kodiakRouter`.

N1-Audit: Redundant initializeV2

Consolidated into main `initialize()`.

Files Modified

Core: 9 files
Interfaces: 1 file
Tests: 6 files
Total: 18 files, ~800 LOC

Verification

Compilation: Success
Tests: Passing
Storage: No layout changes
Compatibility: Backward compatible