Scanned Code Report

AUDITAGENT

Powered by NETHERMIND SECURITY

Code Info

Developer Scan

Scan ID 10	Date February 25, 2026
Organization RigoBlock	Repository v3-contracts
Branch fix/0x-adapter	Commit Hash f0c59f27...36ca352d

Contracts in scope

contracts/protocol/extensions/adapters/A0xRouter.sol

contracts/protocol/extensions/adapters/interfaces/IA0xRouter.sol

Code Statistics

Findings 0	Contracts Scanned 2	Lines of Code 248

Findings Summary

Total Findings

- High Risk (0)
- Medium Risk (0)
- Low Risk (0)
- Info (0)
- Best Practices (1)

Code Summary

This protocol provides an adapter contract, `A0xRouter`, that enables smart pools to execute token swaps through the 0x swap aggregator. It acts as a secure bridge between a pool's funds and the 0x protocol's `AllowanceHolder` and `Settler` contracts, allowing pools to access aggregated decentralized exchange liquidity.

The adapter is designed to be called via `delegatecall` from the main smart pool contract. Before executing a swap, it performs several critical security validations on the calldata provided by the 0x API. These checks include:
- Verifying the authenticity of the 0x Settler contract to prevent interactions with counterfeit contracts.
- Ensuring that the recipient of the swapped tokens is the smart pool itself.
- Confirming that the token being acquired has a valid price feed through an integrated oracle, which is essential for the pool's accounting and risk management.
- Enforcing a strict allowlist of permissible 0x actions, allowing only specific DEX-related functions while blocking potentially dangerous or arbitrary calls.

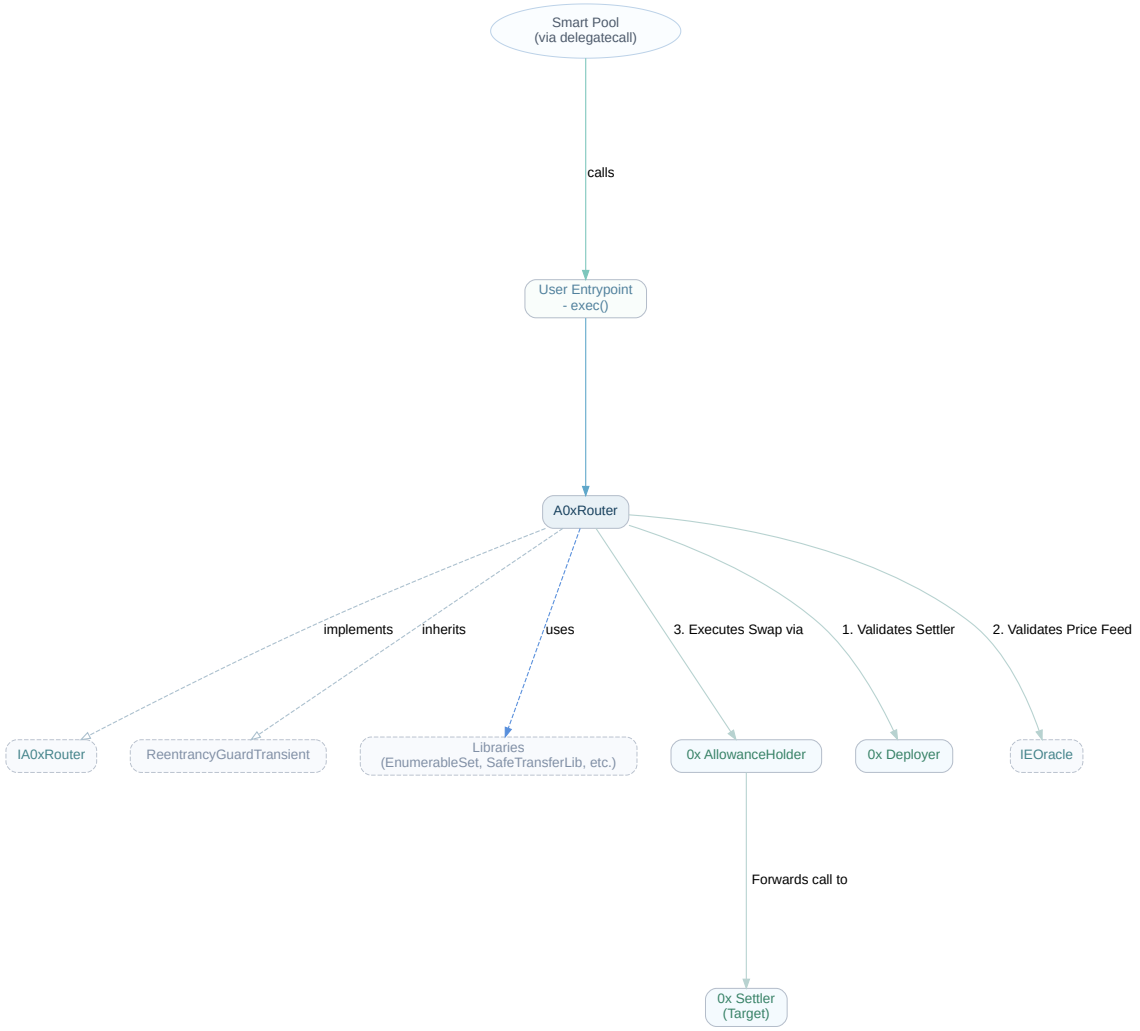
To facilitate the swap, the contract grants a temporary, maximum ERC20 approval to the 0x `AllowanceHolder` for the duration of the transaction. This approval is immediately reduced to a nominal amount upon completion to mitigate security risks associated with hanging approvals.

Actors and Entry Points

The primary actor is the **Smart Pool**, which executes swaps through this adapter.

- `exec(address operator, address token, uint256 amount, address payable target, bytes calldata data)`: Executed by a smart pool via `delegatecall` to perform a token swap using the 0x protocol. It validates the swap parameters and forwards the call to the 0x `AllowanceHolder`.

Code Diagram



1 of 1 Findings

contracts/protocol/extensions/adapters/A0xRouter.sol

Potential Denial of Service via Out-of-Bounds Read in Calldata Parsing

Best Practices

The `_checkActionsAllowed` function decodes multiple offsets from the user-provided `data` calldata to locate the `actions` array and the individual action selectors within it. The function does not perform any bounds checking to ensure that the calculated positions (`elPos`, `selectorPos`) are within the length of the `data` array before attempting to read from them.

```
function _checkActionsAllowed(bytes calldata data) private pure {
    // ...
    uint256 actionsOffset = abi.decode(data[100:132], (uint256));
    uint256 arrStart = 4 + actionsOffset;
    uint256 numActions = abi.decode(data[arrStart:arrStart + 32], (uint256));

    for (uint256 i; i < numActions; ++i) {
        uint256 elPos = arrStart + 32 + i * 32;
        // No check if elPos is within data.length
        uint256 elOffset = abi.decode(data[elPos:elPos + 32], (uint256));
        uint256 selectorPos = arrStart + elOffset + 64;
        // No check if selectorPos + 4 is within data.length
        bytes4 actionSelector = bytes4(data[selectorPos:selectorPos + 4]);
        _assertIsAllowedAction(actionSelector);
    }
}
```

A malicious pool operator could provide a crafted `data` payload with large or invalid offset values. This would cause the EVM to attempt an out-of-bounds read when decoding `elOffset` or slicing `actionSelector`, which would cause the entire transaction to revert. This constitutes a denial-of-service vector, as any swap attempt using such malicious calldata would fail, preventing legitimate swaps.

Disclaimer

Kindly note, no guarantee is being given as to the accuracy and/or completeness of any of the outputs the AuditAgent may generate, including without limitation this Report. The results set out in this Report may not be complete nor inclusive of all vulnerabilities. The AuditAgent is provided on an 'as is' basis, without warranties or conditions of any kind, either express or implied, including without limitation as to the outputs of the code scan and the security of any smart contract verified using the AuditAgent.

Blockchain technology remains under development and is subject to unknown risks and flaws. This Report does not indicate the endorsement of any particular project or team, nor guarantee its security. Neither you nor any third party should rely on this Report in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset.

To the fullest extent permitted by law, Nethermind disclaims any liability in connection with this Report, its content, and any related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. Nethermind does not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and Nethermind will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.