Final Audit Report for ConvexToken Contract

This report summarizes the findings of a multi-tool audit of the ConvexToken contract, utilizing Slither, My

1. Access Control Vulnerability (Medium)

- **Description:** The `updateOperator` function allows anyone to update the operator address to the ope
- **Impact:** If the staker contract is compromised or has a bug, an attacker could gain control of the ope
- **Mitigation:** Restrict access to the `updateOperator` function, ideally by allowing only the current oper

2. Logic Flaw in Mint Function (High)

- **Description:** The `mint` function's logic is complex and depends on variables like `totalSupply`, `redu
- **Impact:** An attacker could manipulate these variables, potentially minting more tokens than intended
- **Mitigation:** Thoroughly audit the `mint` function logic. Consider simplifying the logic and using unit te

3. Potential for Lost Funds (Medium)

- **Description:** The `maxSupply` limit in the `ConvexToken` contract could result in lost funds if attempt
- **Impact:** If a user attempts to mint an amount beyond the `maxSupply`, the excess amount will not be
- **Mitigation:** Consider implementing a mechanism to handle excess minting attempts. This could invo

4. Missing Function Visibility Specifiers (Medium)

- **Description:** Several interface functions lack explicit visibility specifiers (`public`, `external`, `internal`
- **Impact:** If the actual contracts implementing these interfaces incorrectly define visibility specifiers, it
- **Mitigation:** Explicitly define visibility specifiers for all interface functions. Use a consistent convention

5. Arbitrary Function Execution (High)

- **Description:** The `IStaker` interface contains an `execute` function that could allow calling arbitrary fu
- **Impact:** An attacker could exploit this function to call malicious functions on other contracts, potentia
- **Mitigation:** Restrict access to the `execute` function by using a trusted access control mechanism. A

Note: This report focuses on the most critical vulnerabilities identified. It is recommended to conduct a