StackFi Avax Security Review

Introduction

A time-boxed security review of the **StackFi Avax** contracts was conducted by **Stonewall**, with a focus on the security aspects of the smart contract implementation.

Disclaimer

A smart contract security review can never verify the complete absence of vulnerabilities. This is a time, resource and expertise bound effort where we try to find as many vulnerabilities as possible. We can not guarantee 100% security after the review or even if the review will find any problems with your smart contracts. Subsequent security reviews, bug bounty programs and on-chain monitoring are strongly recommended.

About Stonewall

Stonewall is an independent smart contract security firm delivering immovable protection for Web3 protocols. Our team brings deep expertise in DeFi security, having reviewed DEXs, yield farming protocols, gaming contracts, and complex financial systems.

About StackFi Avax

StackFi Avax is a **fork of Gearbox Protocol** adapted for the Avalanche network. It provides leveraged yield farming through:

- **Credit Accounts**: Isolated smart contract accounts for leveraged positions
- **Credit Facade**: User-facing interface for opening/managing positions
- **Pool V3**: Lending pools providing liquidity for leverage
- **Trading Adapters**: Connectors to DEXs (UniswapV2, UniswapV3, Curve)
- **Price Oracles**: Asset price feeds for health factor calculation

Key Differences from Gearbox

StackFi is a minimal fork with the following customizations:

1. **Network Adaptation**: Configured for Avalanche C-Chain
2. **Pool Addresses**: Updated pool and oracle addresses for AVAX ecosystem
3. **Trading Adapter**: Custom adapter for AVAX-specific DEX integrations

Privileged Roles & Actors

Role	Description
Configurator	Can modify pool parameters, add collateral tokens
Controller	Emergency pause, risk parameter adjustments
Adapters	Whitelisted contracts for executing trades

Observations

- Core credit logic unchanged from audited Gearbox V3
- Custom TradingAdapter for Avalanche DEX integration
- Standard ERC4626-style pool implementation

Risk Classification

	High Impact	Medium Impact	Low Impact
High Likelihood	Critical	High	Medium
Medium Likelihood	High	Medium	Low
Low Likelihood	Medium	Low	Low

Security Assessment Summary

Review Details	

Protocol Name	StackFi Avax
Repository	Private
Commit	`1aebbece8db809ecac439fbbfffe94a6c90fe931`
Review Date	January 2026
Methods	Manual review, static analysis
Network	Avalanche C-Chain
Base Protocol	Gearbox Protocol V3

Project Links

Platform	Link
Twitter	@stackfibase
Telegram	Join Telegram
Discord	Join Discord
Farcaster	@stackfi

Base Protocol Security

Gearbox Protocol V3 has undergone extensive auditing:

- **ChainSecurity** - Full protocol audit
- **Sigma Prime** - Credit account and pool review
- **Code4rena** - Competitive audit with $200K+ bounty
- **Immunefi** - Active bug bounty program ($1M+ max)

Scope (Custom Changes Only)

Contract	SLOC	Notes
`TradingAdapter.sol`	~50	Empty/placeholder
`DeployStackFi*.s.sol`	~500	Deployment scripts

Findings Summary

ID	Title	Severity	Status
[L-01]	Deployment scripts contain hardcoded test addresses	Low	Open
[I-01]	TradingAdapter is empty placeholder	Informational	Open
[I-02]	Consider using verified Gearbox deployment	Informational	Open

Findings

[L-01] Deployment scripts contain hardcoded test addresses

Severity: Low

Location: `scripts/DeployStackFi*.s.sol`

Description:

Deployment scripts contain hardcoded addresses that may be test/development addresses. Before mainnet deployment, ensure all addresses are verified for the target network.

Recommendation:

Review and update all hardcoded addresses for Avalanche mainnet before deployment.

[I-01] TradingAdapter is empty placeholder

Severity: Informational

Location: `contracts/TradingAdapter.sol`

Description:

The TradingAdapter contract appears to be an empty placeholder. The actual trading adapter implementation needs to be completed before the protocol is functional.

Recommendation:

Implement the trading adapter with proper security considerations:

- Input validation on all swap parameters

- Slippage protection

- Deadline checks

- Whitelisted DEX addresses only

[I-02] Consider using verified Gearbox deployment

Severity: Informational

Description:

Since StackFi is a Gearbox fork, consider:

1. Using official Gearbox deployment scripts as reference

2. Verifying contract bytecode matches audited versions

3. Running Gearbox's test suite on the fork

Inherited Security Properties

As a Gearbox V3 fork, StackFi inherits these security properties:

Positive (from Gearbox)

- Isolated credit accounts prevent cross-account attacks

- Health factor system prevents under-collateralization

- Multi-sig and timelock on critical operations

- Comprehensive access control via ACL

- Pause functionality for emergencies

- Price oracle redundancy

Considerations for Fork

- Oracle addresses must point to valid Avalanche price feeds

- Adapter allowlists must be configured for AVAX DEXs

- Pool parameters should match AVAX market conditions

- Collateral tokens must be verified for AVAX network

Fork-Specific Recommendations

1. **Verify Oracle Compatibility**

   - Ensure Chainlink feeds exist for all collateral tokens on Avalanche
   - Configure proper staleness thresholds for AVAX block times

2. **Adapter Security**

   - Implement TradingAdapter with proper validation
   - Only whitelist verified DEX contracts
   - Add slippage and deadline parameters

3. **Testing**

   - Run Gearbox's full test suite on fork
   - Add integration tests for AVAX-specific DEXs
   - Simulate liquidation scenarios with AVAX gas costs

4. **Deployment**

   - Use multi-sig for admin functions
   - Implement timelock for parameter changes
   - Consider gradual rollout with caps

Conclusion

StackFi Avax is a fork of the well-audited Gearbox Protocol V3. The core protocol logic inherits the security properties of multiple professional audits.

The main work remaining is:

1. Completing the TradingAdapter implementation
2. Configuring correct Avalanche addresses
3. Testing the integration thoroughly

Since core logic is unchanged from audited Gearbox, risk is primarily in configuration and custom adapters.

Overall Risk Assessment: Low (assuming correct configuration and adapter implementation)

This security review was conducted by Stonewall. For questions or clarifications, contact our team.