



BlockSec

Security Audit Report for Ref-Exchange

Date: Nov 2, 2022

Version: 1.0

Contact: contact@blocksec.com

Contents

1	Introduction	1
1.1	About Target Contracts	1
1.2	Disclaimer	2
1.3	Procedure of Auditing	2
1.3.1	Software Security	2
1.3.2	DeFi Security	3
1.3.3	NFT Security	3
1.3.4	Additional Recommendation	3
1.4	Security Model	3
2	Findings	5
2.1	Software Security	5
2.1.1	Improper Account Unregistration	5
2.2	DeFi Security	6
2.2.1	Unrestricted Referral Account	6
2.2.2	Incorrect Admin Fees Calculation in Simple Pool	7
2.3	Additional Recommendation	9
2.3.1	Lack of Check on Guardians' Removal	9
2.3.2	Two-Step Transfer of Privileged Account Ownership	10
2.3.3	Potential Elastic Supply Token Problem	10
2.3.4	Improper Check on the Admin Fees	10
2.3.5	Lack of Check in retrieve_unmanaged_token()	11
2.3.6	Lack of Check on the Gas Used by migrate()	12
2.3.7	Code Optimization (I)	13
2.3.8	Code Optimization (II)	16
2.4	Notes	17
2.4.1	Delayed Price in Rated Swap Pool	17
2.4.2	Timely Triggering update_token_rate()	18
2.4.3	Sensitive Functions Managed by DAO	18

