Preliminary Notes: AdMonkey

Brewlabs Services Hub

Summary: AdMonkey is a token smart contract for the AdMonkey project. It is written in Solidity and compiled using build 0.8.6. The smart contract supports regenerative tokenomics and allows holders to receive dividends from transactions in BNB or in their nominated choice of token from across a selection of decentralised exchanges.

Audit package: Standard
Contact: 0x9eeb03bbdef40980e16e6f4332f486d991d11b84
Date: 2021-10-19
Status: Deployed to BSC Mainnet

Disclaimer: This audit documentation is for discussion purposes only. The scope of this audit was to analyze and document AdMonkey smart contract codebase for quality, security, and correctness. This audit guarantees that your code has been revised by an expert.

Overview of Audit

No major or medium security issues were identified.
Minor logic issues identified, however work-arounds in place or issues are no longer relevant since the contract has already launched.
Good use of comments.

Security issues

Low level security issued detected:

1. Floating pragma set (^*{solidity compiler version}. If relying on byte-code level verification, best practice is to lock the compiler version prior to deployment.
2. tx.origin (lines 1748, 1842) returns the address of the calling account that sent the transaction. Use of this variable can lead to authorisation bypass vulnerabilities if an authorised account calls into a malicious contract (SWC15). Both contracts where the tx.origin is used are not considered malicious.

Logic issues

1. Taxes (operations, wallet etc) are paid out from the BNB derived from the liquidity pool rather than the BNB gathered in the contract from taxes. However, the recoverExcess (line 1941) and buyBackTokens (line 1925) function allows project developers to withdraw or burn this BNB, respectively.
2. There is no control to prevent holders from accidentally setting their reward token to a wallet address rather than a token contract. Holders will still be paid out dividends, however they will be in BNB rather than their 'reward' token.
3. If a holder is excluded from dividends and then included, they will not receive dividends until the they transact the token. This will then reset their position in the TokenHoldersMap and enable them to receive dividends.
4. The rewardsFee condition (line 1838) prevents holders from receiving dividends when the reward tax is 0. While this is logical, it could be possible for holders to miss out on any dividends that are earned after the SwapBack function is invoked and fi their account is not processed (via the Dividend Tracker) before the rewardsToken is fee is set to 0.
5. Line 1400 is missing the 'true' assignment to enable the owner to trade when trading is disabled. This is no longer relevant since contract has already launched.
6. Return status not checked after transfers to Operations and Team wallets
7. Events not emitted for some functions which change state variables eg. updateSwapEnabled, updateFees. This means only contract owner can alter state variables without the public being aware of changes.

Code Issues

1. Unused code, lines 1871-1873, could be removed.
2. Code refers to Eth (line 1886), could be replaced with BSC.
3. Use inclusive terminology that does not promote negative associations with the colours 'black' or 'white'

Recommendations:

1. Contract allows owners to enable/disable liquidity deposits (swapEnabled) and alter transactions taxes (updateFees) which goes against the ethics of Decentralised Finance and presents a risk to the community. To mitigate risk, ensure the team is doxxed or consider (Know Your Customer) KYC services.
2. Contract allows owners to blacklist wallets (potentially permanently), and to do so with no visibility to public (no event emitted) which goes against the ethics of Decentralised Finance and presents a risk to the community. To mitigate risk, ensure the team is doxxed or consider (Know Your Customer) KYC services.

Conclusion: The Brewlabs team thank you for the opportunity to review and audit your smart contact code. The data from this report will be formalised in the audit publication for your community. Keep in touch as we offer discounts for repeat business and on a range of other services!

The Brewlabs Team.