RomyRom

Audit report

Ermine LaunchPad

Contract address: 0xA74EB1A523B962571e496F868596510C6147BcDB

March 25, 2023

Content

Disclaimer

RomyRom audits various projects where smart contracts are involved. We do not guarantee that the purpose of the project may be fraud, "rug pull", withdrawing liquidity, selling and transferring the project and its team.

An audit of a smart contract is not an offer, investment advice, or a recommendation to buy tokens.

RomyRom is not responsible for any losses and speculative investments. Use the information obtained from this audit for informational purposes.

Do your own research on the project, documentation, and its social media.

Object under study

LaunchPad Ermine

Ermine is developing an ecosystem consisting of virtual mining using virtual miners, a liquidity pool with an exchange, a return system, a referral program, a treasury and interaction with yield smart contracts. The Ermine launchpad was created for the seed round of raising funds for the development of the project. The total limit of Ermine tokens for the seed round is predetermined in the amount of 37,500,000 ERM. Installed SoftCap 20 ETH and HardCap 187.5 ETH. In the event that SoftCap does not take place, the investor will be able to return their ETH.

Initial values and characteristics

Ecosystem – Ethereum

Relationship with Ermine Token Contract

0xda542de613834Ced3c8c1aD9B884f71bc1CbFd06

Pre-sale end date set to Jule 15, 2023 at 23:59 UTC, in the event that HardCap is reached, the pre-sale ends. The pre-sale can be extended by 30 days once.

The fixed price of the token is 0.000005 ETH for 1 ERM.

totalBuy stores the number of sold tokens in the format 1e18.

Calling functions to withdraw the collected Ethereum, withdraw the remaining unsold Ermine tokens, confirm the wallet address for the white list, extend the presale by 30 days require the participation of the administrator address and the owner address. Confirmations are comparable to a multi-signature from two persons.

The user structure can store data on the limits of tokens available for purchase, the date of the last purchase of tokens, the date of unlocking of tokens, the number of tokens sent to the user's address, the number of blocked tokens, a variable for providing access to operations in a smart contract.

Verify of smart contracts

Verified contract source code in browser:

https://etherscan.io/address/0xa74eb1a523b962571e496f868596510c61 47bcdb#code

Contract Name: LaunchPadErmine

Compiler Version: v0.8.17+commit.8df45f5f

Optimization Enabled: Yes with 200 runs

Other Settings: default evmVersion

Contract Source Code Verified (Exact Match)

Checking hashes (SHA256) modules, libraries

File name	SHA256 Checksum	Conclusion
Context.sol	6de5302543723d32c8eaf17becc4525936e16d9c4551455c93d306b9b72c0799	verified
IERC20Metadata.sol	370d2a3f5d1002a531dbe728d6e6c945ee160aecf16d01dc7304a0a534947c8f	verified
ERC20Burnable.sol	8da478d50272b5de7478f70c72d5b573ce12c798a6260402f484eb562a9721d9	verified
IERC20.sol	6654ca211d7ed22937fae539bcf24e0bda89ba7489d4a2f439cc52f53db6ec4d	verified
ERC20.sol	eac10472f2555cd9806352fe9278f6410dc92969b842283ea450db0308a8cc2e	verified
Ownable.sol	96a3b09372173d7174fcb0080a97c0cd9abb51cd31e71ecd597d62e0942cb7c4	verified
Ermine.sol	77ca05bc1f3917e705cb28331962e07c3851b80b57368668a9cbcf98f2a10f5b	verified

Owner: 0x18b5d766C8714BA3280403A1fD5e8e1183B707b8

Control modifiers:

```
//For only Admin
   modifier onlyAdmin() {
   require(msg.sender == adminAddress);
   _;
   }

//Only for confirmed members (whitelisted addresses)
   modifier onlyVerify() {
   require(_user[msg.sender].verify, "Error: Your address has not been verified, is not listed, or has
been deleted after the ETH was returned! Or you have withdrawn all your ERM tokens.");
   _;
   }
```

Functions created by the developer

Below is a study of the functions created by the developer

The Launch.sol file includes 11 functions

Function name	Permissions	Description
addWL (uint256 _limit, uint256 _limitMin, address _wallet)	available to onlyOwner	Adding addresses and their limits for the purchase of tokens to the white list
saleERM()	available for whitelisted addresses	Buying Ermine tokens with Ethereum
unLockErmine()	available for whitelisted addresses	Withdrawal of tokens from storage. Withdrawal is available 90 days after purchase. (The speed of unlocking tokens is 1 ERM in 5 seconds)
returnETH(uint256 _amount)	available for whitelisted addresses	Return with the exchange of tokens back to Ethereum in case SoftCap is not reached.
returnERM()	available to onlyOwner	Withdrawal of Ermine tokens from the contract if SoftCap is not reached.
setTime()	available to onlyOwner	Adding 30 extra days to extend the presale.
withdrawETH()	available to onlyOwner	Withdrawal of collected Ethereum, available upon reaching SoftCap.
withdrawErmineTokens()	available to onlyOwner	Withdrawal of unsold tokens from the contract when SoftCap is reached
getUsers(address _wallet)	Available for everyone to read	Reading a User Data Structure

Conclusion

During the study of the **LaunchPadErmine** contract, no errors were found in the source code. The code audit of the libraries used did not reveal any changes made to them. Library file hashes correspond to stock values.
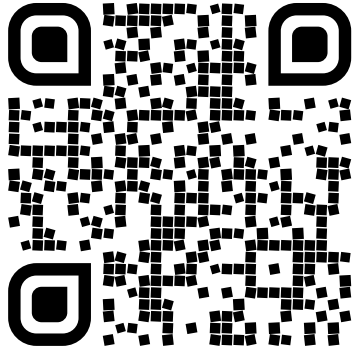
No vulnerabilities were found. The Ermine smart contract has successfully passed security tests and does not pose a threat when used.

Contacts

🌐 https://romyrom.com/en/

🐦 https://twitter.com/RRWeb3