Coinsult

Advanced Manual Smart Contract Audit

Project: Eleia
Website: https://eleia.game

Low-risk	Medium-risk	High-risk
3 low-risk code issues found	1 medium-risk code issues found	0 high-risk code issues found

Contract address
0xa0cD38F5b2d05C4448c5fC614FDcB31f36E5597B

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x6863e714f3773401004e2c901985f85e80e6c575	100,000,000	100.0000%

Source code

Coinsult was commissioned by Eleia to perform an audit based on the following smart contract:

https://bscscan.com/address/0xa0cD38F5b2d05C4448c5fC614FDcB31f36E5597B#code

Manual Code Review

🟢 Low-risk

5 low-risk code issues found.
Could be fixed, will not bring problems.

- Contract contains Reentrancy vulnerabilities:
  Additional information: This combination increases risk of malicious intent. While it may be justified by some complex mechanics (e.g. rebase, reflections, buyback).
  More information: Slither

```
    function _transfer(
        address sender,
        address recipient,
        uint256 amount
    ) internal virtual {
        require(sender != address(0), "BEP20: transfer from the zero
address");
        require(recipient != address(0), "BEP20: transfer to the zero
address");

        _beforeTokenTransfer(sender, recipient, amount);

        uint256 senderBalance = _balances[sender];
        require(senderBalance >= amount, "BEP20: transfer amount
exceeds balance");
        _balances[sender] = senderBalance - amount;
        _balances[recipient] += amount;

        emit Transfer(sender, recipient, amount);
    }
```

- Remove commented code (50%+ of lines is commented)
  Commented code makes the contract messy and hard to read

```
// File: @openzeppelin/contracts/access/Ownable.sol
// File: contracts/token/BEP20/lib/BEP20Operable.sol
```

- Solidity version defined 17 times
  No need to redefine the same solidity version

```
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
pragma solidity ^0.8.0;
```

🟡 Medium-risk

1 medium-risk code issues found.
Should be fixed, could bring problems.

- Owner can mint tokens

```
    /**
     * @dev Function to mint tokens.
     *
     * WARNING: it allows everyone to mint new tokens. Access controls
MUST be defined in derived contracts.
     *
     * @param account The address that will receive the minted tokens
     * @param amount The amount of tokens to mint
     */
    function mint(address account, uint256 amount) public canMint {
        _mint(account, amount);
    }
```

🔴 High-risk

0 high-risk code issues found

Must be fixed, and will bring problems.

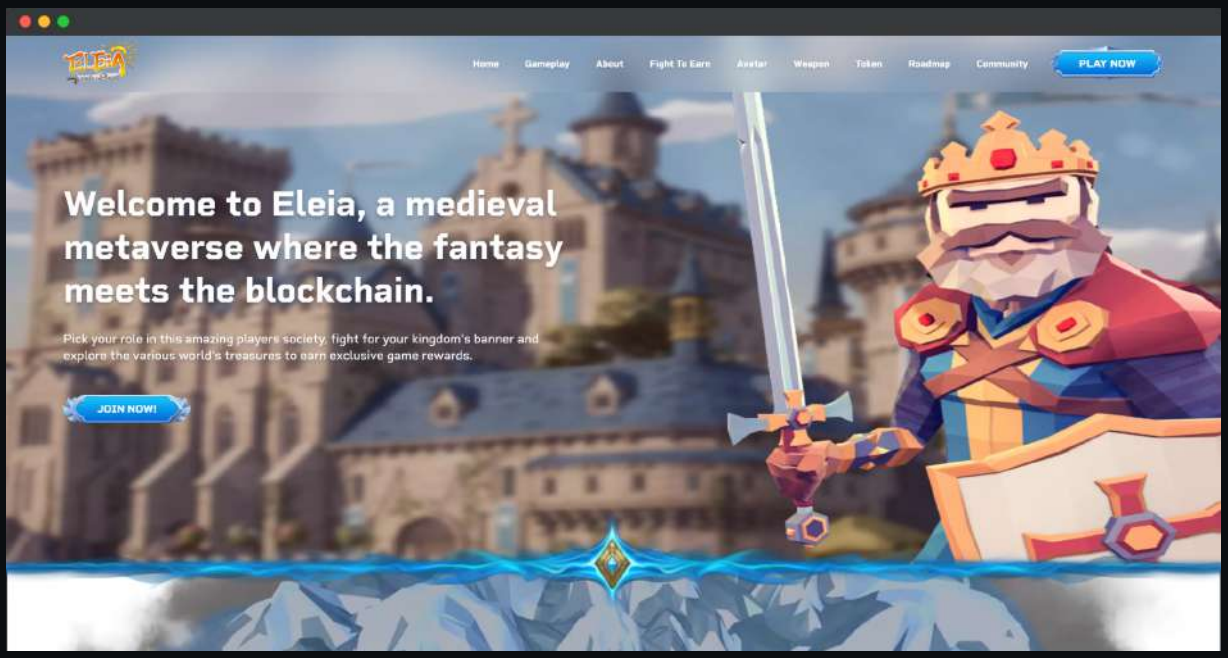
Extra notes by the team

- The ownership of the contract isn't renounced
- The owner can burn tokens
- The owner can mint tokens

Contract Snapshot

```
contract BEP20 is Ownable, IBEP20 {
    mapping(address => uint256) private _balances;

    mapping(address => mapping(address => uint256)) private
_allowances;

    uint256 private _totalSupply;

    string private _name;
    string private _symbol;
    uint8 private _decimals;

    /**
     * @dev Sets the values for {name} and {symbol}, initializes
{decimals} with
     * a default value of 18.
     *
     * To select a different value for {decimals}, use
{_setupDecimals}.
     *
     * All three of these values are immutable: they can only be set
once during
     * construction.
     */
    constructor(string memory name_, string memory symbol_) {
        _name = name_;
        _symbol = symbol_;
        _decimals = 18;
    }

    /**
     * @dev Returns the name of the token.
     */
    function name() public view override returns (string memory) {
        return _name;
    }

    /**
     * @dev Returns the symbol of the token, usually a shorter version
of the
```

Website Review



Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.

- Mobile Friendly
- Contains no jQuery errors
- SSL Secured
- No major spelling errors

Loading speed: 87%

Rug-pull Review

Based on the available information analyzed by us, we come to the following conclusions:

🟡 Locked Liquidity (no liquidity yet)

🟡 Large unlocked wallets (tokens not distributed yet)

🟡 No doxxed Team (yet)

Honeypot Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Ability to sell

🟢 Owner is not able to pause the contract

🟢 Router can not be changed

Note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.