Coinsult

Advanced Manual Smart Contract Audit

Project: Times
Website: http://timesdao.co/

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

Contract address
0x2F462fe879B699897b2ef3c870bFEB24eD7Ba492 (heco)

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 checks the contract for coding issues, we do not guarantee the use case of the code. We do not check the logic of the functions and if they are used for what they were intended to be used.

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

Tokenomics

Rank	Address	Quantity	Percentage
1	0x144b7769f30f9f6d93bf8ee95f28b90ebbbf441d	50,308,773.701193641063879198	25.1544%
2	Null Address: 0x000...dEaD	24,008,149.031466710373378868	12.0041%
3	0x9d5882cfa95059f2db56f9559c2e1d4cacf964cd	5,521,488.476208672569483784	2.7607%
4	0xdd99b6e86c62f42431115020356ce9ef9422b483	1,899,505.343520505860765797	0.9498%
5	0x371ea947c5f5a9a11f386953785649bbcbd9457c	1,869,370.383733117866362579	0.9347%
6	0xf9ac725fd03c85145455322340ce578bc2a66232	1,851,853.972552737277813179	0.9259%
7	0x975d652fcb7cee452cc81a35bf936cf38a589368	1,512,685.873761008758899588	0.7563%
8	0xeabb3067779b6fbec4a964a82c97f62bbd30a064	1,386,382.090543368497012607	0.6932%
9	0xc080255123dfd1a735c5c8c7ee0ff1d7c0f1543d	1,322,564.663279760213763415	0.6613%
10	0x94d636093d3b7b5ef17a089431bfc12db884df6f	1,256,221.39922357636096967	0.6281%

Source code

Coinsult was commissioned by Times to perform an audit based on the following smart contract:
https://hecoinfo.com/address/0x2f462fe879b699897b2ef3c870bfeb24ed7ba492#code

Manual Code Review

🟢 Low-risk

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

- Literals with many digits are difficult to read and review.
  Recommendation: Use Ether suffix, Time suffix, or The scientific notation

```
    uint256 private _tTotal = 200000000 * 10**18;
```

- The return value of an external transfer/transferFrom call is not checked
  Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

  More information:
  https://github.com/crytic/slither/wiki/Detector-Documentation#unchecked-transfer

```
IERC20(husdtToken).transfer(address(devAddress), dividends);
```

- Missing events for critical arithmetic parameters
  Emit an event for critical parameter changes.

```
    function excludeFromFee(address account) public onlyOwner {
        _isExcludedFromFee[account] = true;
    }

    function includeInFee(address account) public onlyOwner {
        _isExcludedFromFee[account] = false;
    }

    function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
        _taxFee = taxFee;
    }

    function setLiquidityFeePercent(uint256 liquidityFee) external
onlyOwner() {
        _liquidityFee = liquidityFee;
    }

    function setBurnFeePercent(uint256 burnFee) external onlyOwner() {
        _burnFee = burnFee;
    }

    function setDevFeePercent(uint256 devFee) external onlyOwner() {
        _devFee = devFee;
    }

    function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner()
{
        _maxTxAmount = maxTxPercent;
    }
```

- Contract contains Reentrancy vulnerabilities:

```
function _transfer(
    address from,
    address to,
    uint256 amount
) private {
    require(from != address(0), "ERC20: transfer from the zero address");
    require(to != address(0), "ERC20: transfer to the zero address");
    require(amount > 0, "Transfer amount must be greater than zero");
    if(from != ownerAddres && to != ownerAddres) {
        require(amount <= _maxTxAmount, "Transfer amount exceeds the maxTxAmount.");
    }
    // also, don't swap & liquify if sender is uniswap pair.
    uint256 contractTokenBalance = balanceOf(address(this));

    if(contractTokenBalance >= _maxTxAmount)
    {
        contractTokenBalance = _maxTxAmount;
    }

    bool overMinTokenBalance = contractTokenBalance >= numTokensSellToAddToLiquidity;
    if (
        overMinTokenBalance &&
        !inSwapAndLiquify &&
        to == uniswapV2Pair &&
        swapAndLiquifyEnabled
    ) {
        contractTokenBalance = numTokensSellToAddToLiquidity;
        //add liquidity
        swapAndLiquify(contractTokenBalance);
    }

    //indicates if fee should be deducted from transfer
    bool takeFee = true;

    //if any account belongs to _isExcludedFromFee account then remove the fee
    if(_isExcludedFromFee[from] || _isExcludedFromFee[to]){
        takeFee = false;
    }

    //transfer amount, it will take tax, burn, liquidity fee
    _tokenTransfer(from,to,amount,takeFee);
}
```

- Remove commented code
  Remove commented code for better readability and optimization of the contract

```
    /**
     * @dev Moves `amount` tokens from `sender` to `recipient` using
the
     * allowance mechanism. `amount` is then deducted from the caller's
     * allowance.
     *
     * Returns a boolean value indicating whether the operation
succeeded.
     *
     * Emits a {Transfer} event.
     */
    function transferFrom(address sender, address recipient, uint256
amount) external returns (bool);
```

🟡 Medium-risk

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

🔴 High-risk

0 high-risk code issues found
Must be fixed, and will bring problems.

Extra notes by the team

- Owner can change the buy and sell fees without a limit
- Owner can exclude from fees
- Owner can set max transaction amount without a limit
- The ownership of the contract isn't renounced

Contract Snapshot

```
contract token is Context, IERC20, Ownable {
    using SafeMath for uint256;
    using Address for address;

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

    mapping (address => bool) private _isExcludedFromFee;

    uint256 private constant MAX = ~uint256(0);
    uint256 private _tTotal = 200000000 * 10**18;
    uint256 private _rTotal = (MAX - (MAX % _tTotal));
    uint256 private _tFeeTotal;

    string private _name = "TIMES";
    string private _symbol = "TIMES";
    uint8 private _decimals = 18;

    uint256 public _taxFee = 0;
    uint256 private _previousTaxFee = _taxFee;

    uint256 public _liquidityFee = 3;
    uint256 private _previousLiquidityFee = _liquidityFee;

    uint256 public _burnFee = 1;
    uint256 private _previousBurnFee = _burnFee;

    uint256 public _devFee = 1;
    uint256 private _previousDevFee = _devFee;

    address public burnAddress =
address(0x000000000000000000000000000000000000dEaD);
    address public ownerAddres =
address(0x26a33f809b0002778C69CfF071baE144E742690F);
    address public devAddress =
address(0x3B3e79849de114f7C045835b6265749A3fdA1b62);
```

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
- 🟡 Not SSL Secured
- 🟢 No major spelling errors

Note: Website is not SSL secured, do not enter personal data on this website.

Loading speed: 78%