MaxiMine Token (MXM) Security Audit

MaxiMine Token (MXM) security audit, conducted by the Callisto Network Security Department in July 2019.

MaxiMine (MXM) Specificities

Audit Request

Audit Top 200 CoinMarketCap tokens.

Maximine Coin (MXM).

https://maximine.io/

Source Code:

https://etherscan.io/address/0x8e766f57f7d16ca50b4a0b90b88f6468a09b0439#code

Disclosure policy:

Public.

Platform:

ETH.

Number of lines:

88.

MaxiMine (MXM) Smart Contract Security Audit Report

Are Your Funds Safe?

1. In scope

- MXM.sol

2. Findings

In total, **5 issues** were reported including:

- 4 low severity issues.
- 1 owner privilege (the ability of an owner to manipulate contract, may be risky for investors).

No critical security issues were found.

2.1. Known vulnerabilities of ERC-20 token

Severity: low.

Description:

1. It is possible to double withdrawal attack. More details here.
2. Lack of transaction handling mechanism issue. WARNING! This is a very common issue and it already caused millions of dollars losses for lots of token users! More details here.

Recommendation:

Add the following code to the `transfer(_to address, ...)` function:

```
require( _to != address(this) );
```

2.2. ERC20 Compliance — event missing

Severity: low.

Description:

According to ERC20 standard when coins are minted(or burned) a `Transfer` event should be emitted.

Code snippet:

- Line 41, 163, 181.

2.3. ERC20 Compliance — transfer returns

Severity: low.

Description:

According EIP20 Standard the `transfer` function should returns boolean value

`function transfer(address _to, uint256 _value) public returns (bool success)` . But here it is not implemented.

Code snippet.

- Line 76.

2.4. ERC20 Compliance: zero-value transfers rejecting

Severity: low.

Description:

EIP20 says that:

> **Transfers of 0 values MUST be treated as normal transfers and fire the Transfer event.**
> **But in this contract, function `transfer` has a condition:**

```
require(balanceOf[_to] + _value > balanceOf[_to]);
```

Code snippet:

- Line 56.

2.5. Owner Privileges

Severity: owner privileges.

Description:

The contract owner allowed to ban transfer functions for certain user.

Code snippet:

- Line 86, 77, 111, 128.

3. Conclusion

The audited smart contract can be deployed. Only low severity issues were found during the audit.

4. Revealing audit reports

- https://gist.github.com/yuriy77k/47daa3e68f380c48e40ff1d101b83d64
- https://gist.github.com/yuriy77k/d59b2a1e8b4801fff49b18b6456d7435
- https://gist.github.com/yuriy77k/f5baefc0963cc674897d5f81413fa605

Appendix

Smart Contract Audits by Callisto Network.

Miscellaneous

Why Audit Smart Contracts?

Our Most Popular Audit Reports.

Trust the Blockchain, Audit the Smart Contracts.

Follow Callisto's Security Department on Twitter to get our latest news and updates!

Published on **October 21, 2020**

Security Audits

‹ Previous post

Next post ›

Callisto Network LTD

71-75 Shelton Street
London, Greater London
United Kingdom, WC2H 9JQ

Join Our Community

Resources

FAQ
Timeline
Airdrop
Community Guidelines

Callisto

Partners

Our GitHub repositories

Media Kit

Contact us

Want to sell your CLO coins OTC?