ETHOS AUDIT

Meme Lordz ($LORDZ)

Crypto & Cyber Security Audit Report

SEP 23, 2021

POWERED BY

DARKSCOPE

Contents

Executive Summary

Audit Details

Project Name	Meme Lordz
Codebase	https://bscscan.com/address/0x2541be91fe0d220ffcbe65f11d88217a87a43bda#contracts
Source Code	MemeLordz.sol
Initial Audit Date	Sept. 23, 2021
Methodology	Manual, Automated

Methodology

This audit's objectives are to evaluate:

- Security-related issues
- Code quality
- Relevant documentation
- Adherence to specifications
- Adherence to best practices
- Cyber-security risks

This audit examines the possibility of issues existing along the following vectors (but not limited to):

- Single & Cross-Function Reentrancy
- Front Running (Transaction Order Dependence)
- Timestamp dependence
- Integer Overflow and Underflow
- Mishandled exceptions and call stack limits
- Security of external calls
- Number rounding errors
- DoS with (Unexpected) Revert
- DoS with Block Gas Limit
- Insufficient gas griefing
- Forcibly sending native currency
- Logical oversights
- Access control
- Centralization of power
- Logic-Specification Contradiction
- Functionality duplication
- Malicious token minting

The code review conducted for this audit follows the following structure:

1. Review of specifications, documentation to assess smart contract functionality
2. Manual, line-by-line review of code
3. Code's adherence to functionality as presented by documentation
4. Automated tool-driven review of smart contract functionality
5. Assess adherence to best practices
6. Provide actionable recommendations

Risk Levels

LOW

The issue is informational and does not pose an immediate risk, but is relevant to security best practices.

MEDIUM

The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.

HIGH

The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.

EXTREME

The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.

Issues Summary

Severity	Unresolved	Acknowledged	Resolved
Extreme	0	0	0
High	0	0	0
Medium	0	1	0
Low	0	1	0

Contract Details

Contract ID	0x2541be91fe0d220ffcbe65f11d88217a87a43bda
Network	BSC
Language	Solidity
Compiler	v0.5.16+commit.9c3226ce
Verification Date	Jun. 18, 2021
Contract Type	BEP-20 Token
Libraries	Custom

Token Details

Contract Name	Meme Lordz
Symbol	$Lordz
Decimals	9
Total Supply	100,000,000

Functions

Function	Parameters	Visibility	Modifiers	Returns	Requires	Events	Called By
constructor		public				Transfer	
getOwner		external	view	address			
decimals		external	view	uint256			
symbol		external	view	string			
name		external	view	string			
totalSupply		external	view	uint256			
balanceOf	address account	external	view	uint256			
transfer	address recipient, uint256 amount	external	view	bool			
allowance	address _owner, address spender	external	view	uint256			
approve	address _owner, address spender	external		bool			
transferFrom	address sender, address recipient, uint256 amount	external		bool			
increaseAllowance	address spender, uint256 addedValue	public		bool			
decreaseAllowance	address spender, uint256 subtractedValue	public		bool			
_transfer	address sender, address recipient, uint256 amount	internal			sender != address(0), recipient != address(0)	Transfer	transfer(), trasferFrom()
_approve	address owner, address spender, uint256 amount	intneral			owner != address(0), spender != address(0)	Approval	approve(), transferFrom(), increaseAllowance, decreaseAllowance

Global Variables

Variable	Type	Visibilty	Read by Functions	Written by Functions
_balances	mapping (address => uint256)	private	balanceOf(), _transfer()	constructor(), _transfer()
_allowances	mapping (address => mapping (address => uint256))	private	allowance(), transferFrom(), increaseAllowance()	_approve
_totalSupply	uint256	private	constructor(), totalSupply()	constructor()
_decimals	uint8	public	_decimals()	constructor()
_symbol	string	public	symbol()	constructor()
_name	string	public	name()	constructor()

Balance Updates

Function	Changes
constructor	_balances[msg.sender] = _totalSupply
_transfer	_balances[sender] = _balances[sender].sub(amount…) _balances[recipient] = _balances[recipient].add(amount)

Summary of Findings

ID	Description	Severity	Status
ETH-1	Use of non-standard SafeMath library	Medium	Acknowledged
ETH-2	Allowance double-spend exploit	Low	Acknowledged

Detailed Findings

ETH-1 – Use of non-standard SafeMath library

Severity: Medium **Status**: Acknowledged

Description: The contract uses a non-standard version of the SafeMath library which may lead to possible integer overflow/underflow scenarios.

Risk: This can become a potentially critical scenario during variable updates which have the potential to exceed the limits of an integers upper or lower bounds. If an integer variable's value exceeds its max value during execution, the variables value will cycle back to either its min/max value, making the entire smart contract more vulnerable to attack.

In this specific scenario, since the only values being updated is the array of _balances, and since the total supply of $Lordz can never exceed the max of uint256, there is relatively lower risk than.

Recommendation: It is highly recommended to use the OpenZeppelin SafeMath.sol library to mitigate the potential overflow/underflow instances.

Update: The team has acknowledged this risk and since the effort in redeploying and redistributing tokens far outweighs the potential risk in this specific case, it will remain acknowledged.

ETH-2 – Allowance double-spend exploit

Severity: Low **Status**: Acknowledged

Description: As with all other ERC-20/BEP-20 smart contracts, they are vulnerable to the allowance double-spend exploit if the use of the approve()/transferFrom() functions are not also careful to reset the allowance to 0 first and verify if it was used before setting a new value.

Risk: A bad actor may be able to submit a transaction prior to an allowance change, making it possible to use the transferFrom() function to send the initial allowance of tokens, and again be able to send the new amount of tokens after the allowance update.

Recommendation: This exploit is mitigated through the use of increaseAllowance()/decreaseAllowance() functions, which update allowances relative to its current value. Users and developers should be made aware of the issue and asked to increase/decrease allowance within their dApps and usage.

Update: The team has acknowledged this risk and will keep developers and users aware.

Automated Analysis

An automated analysis was completed by running Slither on the codebase. A total of 18 issues were detected, however, none of the issues were serious enough to be considered relevant to the security of the smart contract.

Local Variable Shadowing

```
MemeLordz.allowance(address,address).owner (Lordz.sol#203) shadows:
        - Ownable.owner() (Lordz.sol#123-125) (function)
MemeLordz._approve(address,address,uint256).owner (Lordz.sol#237) shadows:
        - Ownable.owner() (Lordz.sol#123-125) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
```

Dead Code

```
Context._msgData() (Lordz.sol#41-44) is never used and should be removed
SafeMath.div(uint256,uint256) (Lordz.sol#82-84) is never used and should be removed
SafeMath.div(uint256,uint256,string) (Lordz.sol#86-93) is never used and should be removed
SafeMath.mod(uint256,uint256) (Lordz.sol#96-98) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Lordz.sol#100-103) is never used and should be removed
SafeMath.mul(uint256,uint256) (Lordz.sol#68-80) is never used and should be removed
SafeMath.sub(uint256,uint256) (Lordz.sol#56-58) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
```

Variable Naming Convention

```
Variable MemeLordz._decimals (Lordz.sol#157) is not in mixedCase
Variable MemeLordz._symbol (Lordz.sol#158) is not in mixedCase
Variable MemeLordz._name (Lordz.sol#159) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-
naming-conventions
```

Redundant Statements

```
Redundant expression "this (Lordz.sol#42)" inContext (Lordz.sol#34-45)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
```

Too many digits

```
MemeLordz.constructor() (Lordz.sol#161-169) uses literals with too many digits:
        - _totalSupply = 100000000000000000 (Lordz.sol#165)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

Gas Optimization

```
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (Lordz.sol#133-136)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (Lordz.sol#138-140)
increaseAllowance(address,uint256) should be declared external:
        - MemeLordz.increaseAllowance(address,uint256) (Lordz.sol#218-221)
decreaseAllowance(address,uint256) should be declared external:
        - MemeLordz.decreaseAllowance(address,uint256) (Lordz.sol#223-226)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-
declared-external
```

Code Documentation

There is little to no commenting within the code nor any additional documentation. While it is not a great need in this specific scenario, it is strongly recommended to document usage, assumptions and future plans.

Adherence to Specifications

The smart contract adheres to the standard BEP-20 token conformity.

Adherence to Best Practices

The smart contract adheres to the majority of best practices associated with a standard BEP-20 token aside from the relatively minor issues described within the findings of this report.

Darkscope Cyber Security Analysis

Cyber Threat Scan

This Cyber Scan report is an examination of the risk profile of cyberspace on behalf of the organisation. This scan presents a snapshot profile of the external cyber risk, as it was conducted over a short period of time, usually days. The information gathered from the internet, social media and the darkweb about the organisation is not exhaustive or complete, due to the continuous growth of cyberspace, its size and the constantly changing nature of focus of the darkweb, particularly. A more comprehensive understanding requires longer monitoring with a broader scope, such as that provided by Darkscope's Cyber Threat Sentinel or Cyber Watchtower services.

Darkscope delivers this report with all due diligence and best efforts but cannot guarantee its accuracy.

This section is in four parts:

1. The Cyber Interference Risk Score provides an overall rating of the cyber risk for the organization.
2. The Cyber Threat Sentinel results rate the risk to the organization from key areas of cyber-attack – phishing, DDoS and Ransom DDoS, website hijacking and ransomware. These are prevalent forms of attack against an organization, its partners, and customers. Understanding these risks can help an organization prepare itself against these forms of attack.
3. Warnings and alerts. Using a traffic light system: Green – information, Orange – warnings, Red – alerts; these items require action to mitigate weaknesses or risks to the organization.
4. Available Information. This information is in cyberspace. It may include emails of former employees or contracts that are no longer current or show infrastructure links that can be exploited (DDoS) that may have weak security or is redundant.

Darkscope Cyber Interference™ Risk Score

This score is a summary of your overall cyber risk. It is compiled from all the risk data Darkscope collects across the internet, social media and the darkweb about you and profiles your organisation within your industry sector and geographic region. Using baseline data collected across millions of data points daily and algorithms that compares your risk factors, your Cyber Interference Risk Score is the most reliable overall assessment of the specific cyber risk for your organisation.

Darkscope provides CIRS with more detail as part of its other enterprise cyber intelligence services. When included in Cyber Threat Sentinel and Cyber Watchtower services it includes more detail such as Partner Risk Score, Darkweb Risk Level, Impersonate and Social Media Sentiment Rating.

Meme Lordz has an average CIRS score and is within it is expected industry and location range. This means Demo has a normal footprint in cyberspace and an average risk of being attacked, compared with other businesses in its region and industry.

A Moderate Cyber Interference Risk Score indicates external interest in the organisation, region, or industry and that the organisation is being examined. Threat actors always have an increased interest in Public Entities like Demo. It is recommended to adjust the Cyber Security Program to mitigate the findings from this report.

Cyber Threat Sentinel Results

The Cyber Threat Sentinel results identifies risk across four key cyber risk areas: Phishing, DDoS/RDDoS, Website Hijacking, and Ransomware and the BEP-20's conformity. The rating scale is Low – Medium – High – Extreme. Each threat type explains how it is determined, your result and how you should interpret or react when the risk is high.

PHISHING ATTACK

To calculate the risk of a phishing attack, we use the information an attacker has or could find in cyberspace about Demo's people, roles, and internal processes. We incorporate past breaches, current cyber-attacks, and campaigns to determine how likely is it that an attacker would choose Demo as a target.

We have identified a Low risk for Meme Lordz based on the analysis we did

DDoS & RDDoS ATTACK

Our system analyses the customer external-facing infrastructure using a black-box approach. This means we simulate what an attacker would be able to find in cyberspace about Demo. This includes domains, sub-domains, applications, and existing protections such as Web application firewalls or load balancers. We also include the location of services and determine the local readiness for DDoS attacks. Smaller countries like New Zealand, for example, have often limited preventive measures available due to its location and internet capabilities when compared with Germany or the US.

We have identified a Medium risk for Meme Lordz based on the analysis we did.

WEBSITE HIJACK

Our system analysis the customer external-facing infrastructure from a black-box approach. This means we simulate what an attacker would be able to find in cyberspace about Demo. This includes domains, sub-domains, applications, and existing protections such as Web application firewalls or load balancers. Out of this information, we determine how vulnerable a customer might be.

We have identified that Meme Lordz has a Medium-High risk of being attacked due to the application WordPress and used AddOns we have found. It is always recommended to review all external-facing applications and perform a penetration test of those to ensure there are no vulnerabilities.

RAMSOMWARE

To calculate the risk of Ransomware attacks, we correlate all available information and create a risk profile containing staff, product/service, and business information. Ransomware is most likely to be successful if the attacker knows about the internal processes and communications of the target. We compare this profile with thousands of other businesses in the same industry and region to create a risk value.

Meme Lordz has a LOW risk of being targeted with ransomware.

Cyber Risks

These Cyber Risks are rated using a Traffic Light system.

Red is an alert. This indicates an imminent risk to the organisation that requires action to fix, prevent or mitigate.

Orange is a warning. These identified risks should be included in a risk register and work program to update, change, or replace.

Green is relevant information. These items show out-of-date practices, expired or end-of-life tools or software. Items identified should be updated or replaced, as they can become vulnerabilities if not fixed.

RISK LEVEL	IDENTIFIED RISK	NOTES AND RECOMMENDATIONS
	INFO: All of the tested domains support TLS 1.3	All of the tested domains support TLS version 1.3
	Warning: The web site domain memelordz.io has directory listing enabled	Our test shows that the domain memelordz.io has the directory listing enabled. This increase the risk for application attacks, especially when WordPress is used. *We recommend that you review the current configurations and disable obsolete functions.*
	Warning: The web site domain memelordz.io uses an outdated plugin	Our test shows that the domain memelordz.io uses an outdated plugin *We recommend that you review the current configurations and update all plugins and the core system as soon as possible.*
	The domain memelordz.com has been identified as too similar to memelordz.io	Our tests show that the domain memelordz.com is very similar in terms of content and industry and the risk of misidentification is high. *We recommend to review this finding and determine the best course of action.*

RISK LEVEL	IDENTIFIED RISK	NOTES AND RECOMMENDATIONS
	Warning: The website memelordz.io uses a plugin: XML-RPC	Our test shows that the domain memelordz.io might use the function XML-RPC. *We recommend that you review the current configurations and disable this function if possible (see Why You Should Disable Xmlrpc.php).*
	Warning: The domain memelordz.io has no DMARC record	Our tests show that the domain memelordz.io has no DMARC record enabled. *We recommend to review this finding and to add a DMARC record to the DNS configuration.*

Available Information - Email Addresses

Publicly available email addresses are a normal part of every organisation's external-facing operation. They are used in marketing, publicity and engaging customers and the public. The cyber risk they represent is that they provide a list of targets for phishing or scam emails and can also be spoofed to scam or phish your customers, partners, or staff. Knowing which emails are public lets you make these people aware of their heightened risk of becoming a target and to be more diligent and capable of identifying unusual or suspicious behaviour and activity.

Email	Name	Position	Department
info@memelordz.io			

Available Information – Infrastructure

Information associated with the hostname, such as IP addresses, DNS and Netblock owner, can provide an attacker with a point of entry (brute force or weak login/password) or a less protected point of attack (DDoS). Ensuring all your IP addresses are well protected will reduce the effect of any attack or breach attempt.

For this report, Darkscope has analysed the public available domains and subdomains. Most of the domains found are hosted in New Zealand, which increases the risk of DDoS / Ransom DDoS attacks as NZ does not have the necessary bandwidth to protect against large scale attacks. Also, it is known in the 'scene' that most NZ businesses are not prepared against DDoS attacks.

Hosts

Hostname	IP Address	Type	Reverse DNS	Netblock Owner
memelordz.io	110.232.143.28	A	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
ns2.syd6.hostingplatform.net.au.	223.130.24.240	NS	ns2.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
ns1.syd6.hostingplatform.net.au.	110.232.143.240	NS	ns1.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD

0 mail.memelordz.io.	110.232.143.28	MX	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
autodiscover.memelordz.io		A		
cpanel.memelordz.io	110.232.143.28	A	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
cpcalendars.memelordz.io	110.232.143.28	A	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
cpcontacts.memelordz.io	110.232.143.28	A	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
webdisk.memelordz.io	110.232.143.28	A	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD
webmail.memelordz.io	110.232.143.28	A	s04fd.syd6.hostingplatform.net.au	SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD

Appendix

Why You Should Disable Xmlrpc.ph

The most significant issues with XML-RPC are the security concerns that arise. The problems aren't with XML-RPC directly, but instead how the file can be used to enable a brute force attack on your site.

Sure, you can protect yourself with incredibly strong passwords and WordPress security plugins. But, the best mode of protection is to simply disable it.

There are two main weaknesses to XML-RPC which have been exploited in the past.

The first is using brute force attacks to gain entry to your site. An attacker will try to access your site using xmlrpc.php by using various username and password combinations. They can effectively use a single command to test hundreds of different passwords. This allows them to bypass security tools that typically detect and block brute force attacks.

The second was taking sites offline through a DDoS attack. Hackers would use the pingback feature in WordPress to send pingbacks to thousands of sites instantaneously. This feature in xmlrpc.php gives hackers a nearly endless supply of IP addresses to distribute a DDoS attack over.

To check if XML-RPC is running on your site, then you can run it through a tool called XML-RPC Validator. Run your site through the tool, and if you get an error message, then it means you don't have XML-RPC enabled.

If you get a success message, then you can stop xmlrpc.php with one of the two approaches below.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.