

ABRACADABRA MONEY · SECURITY REVIEW

Abracadabra Money MagicGLP Upgrade.

A security review of MagicGLP Upgrade.

CLIENT	PROJECT	AUDITORS	AUDIT WINDOW	FINAL REPORT
Abracadabra Money	MagicGLP Upgrade	Guardian	July 31 – August 6, 2025	August 6, 2025

§ 00

Contents.

20 pages: overview, confidence ranking, scope, 11 findings, disclaimer, and about Guardian.

§ 01	Overview	P. 03
§ 02	Confidence Ranking	P. 04
§ 03	Scope & Classifications	P. 05
§ 04	Findings	P. 06
	Main Review · 11 findings	P. 07
§ 05	Disclaimer	P. 19
§ 06	About Guardian	P. 20

§ 01

Overview.

Guardian reviewed MagicGLP Upgrade across a single review round. The final report includes 1 High, 10 Low findings.

AUDIT FIRM	REPOSITORY
Guardian	https://github.com/Abracadabra-money/abracadabra-money-contracts
CLIENT	METHODOLOGY
Abracadabra Money	Smart contract · Manual · Main Review
PROJECT	MAIN REVIEW COMMIT
MagicGLP Upgrade	db69940c51f7
PREPARED BY	
Guardian	
AUDIT WINDOW	
July 31 – August 6, 2025	
FINAL REPORT	
August 6, 2025	

1.1 Confidence Ranking

4 / 5

High Confidence

Guardian assigns a Confidence Ranking of 4 out of 5, combining finding severity, remediation outcome, and the reviewer’s assessment of latent risk. The full scale is on the next page.

1	2	3	4	5
VERY LOW CONFIDENCE	LOW CONFIDENCE	MODERATE CONFIDENCE	HIGH CONFIDENCE	VERY HIGH CONFIDENCE

1.2 Findings at a Glance

SEVERITY	TOTAL	PENDING	ACK	PARTIAL	RESOLVED
● Critical	0	0	0	0	0
● High	1	0	0	0	1
● Medium	0	0	0	0	0
● Low	10	0	6	0	4
● Informational	0	0	0	0	0
All severities	11	0	6	0	5

§ 02

Confidence Ranking.

Guardian assigns a project-level confidence score using the scale below. The ranking combines finding severity, remediation outcome, and the reviewer's assessment of latent risk.

CONFIDENCE RANKING	DEFINITION AND RECOMMENDATION	RISK PROFILE
5 Very High Confidence	Codebase is mature, clean, and secure. No High or Critical vulnerabilities were found. Follows modern best practices with high test coverage and thoughtful design. Recommendation: code is highly secure at time of audit.	0 High/Critical findings and few Low/Medium severity findings.
4 High Confidence ASSIGNED	Code is clean, well-structured, and adheres to best practices. Design patterns are sound and test coverage is strong. Recommendation: suitable for deployment after remediations; consider periodic review with changes.	0-1 High/Critical findings per engagement week and little to no Medium severity findings.
3 Moderate Confidence	Code is functional but shows gaps in defensive programming or test coverage. Recommendation: remediate the findings and re-review the changes before deployment.	Some High/Critical findings, with various Medium severity findings.
2 Low Confidence	Recurring issues suggest systemic gaps rather than isolated mistakes. Recommendation: remediate, then commission a follow-up review at a frozen commit.	Over 6 High and Critical findings across the engagement.
1 Very Low Confidence	The volume and severity of findings indicate the codebase is not ready for production. Recommendation: substantial rework, then a full re-review.	Over 12 High and Critical findings across the engagement.

§ 03

Scope & Classifications.

Guardian reviewed MagicGLP Upgrade in <https://github.com/Abracadabra-money/abracadabra-money-contracts>.

3.1 Severity Matrix

	IMP · HIGH	IMP · MED	IMP · LOW
LIK · HIGH	Critical	High	Medium
LIK · MED	High	Medium	Low
LIK · LOW	Medium	Low	Low

IMPACT · HIGH

Significant loss of assets, harm to a group of users, or core protocol functionality is disrupted.

IMPACT · MEDIUM

Small amount of funds can be lost, or ancillary functionality is affected. Users may experience reduced or delayed receipt.

IMPACT · LOW

Unexpected behavior in some functionality that is notable but does not meet the criteria for higher severity.

LIKELIHOOD · HIGH

Possible with reasonable assumptions that mimic on-chain conditions; cost is low compared to amount gained.

LIKELIHOOD · MEDIUM

Possible only in uncommon cases or requires a large amount of capital relative to disruption caused.

LIKELIHOOD · LOW

Unlikely to ever occur in production.

§ 04

Findings.

Grouped by round. Visible IDs reset by severity within each round, so a finding is named the same way in the report as it was in the channel it was written in. Status is where each finding ended up; its own page says how.

ID	TITLE	CATEGORY	SEVERITY	STATUS	PAGE
MAIN REVIEW					
H-01	Bad Debt Created By The Last Claimer	Gaming	HIGH	RESOLVED	p. 7
L-01	Zero Reward Claims DoS Claims	DoS	LOW	RESOLVED	p. 9
L-02	totalAssets Functions Unexpectedly	Unexpected Behavior	LOW	ACKNOWLEDGED	p. 10
L-03	Callback Claim Tokens Exploit The System	Callbacks	LOW	RESOLVED	p. 11
L-04	Blacklisted Callee Safety Measure	Warning	LOW	ACKNOWLEDGED	p. 12
L-05	Asset Edit Dangers	—	LOW	ACKNOWLEDGED	p. 13
L-06	GLP Yield Unclaimed	Warning	LOW	RESOLVED	p. 14
L-07	0 Shares Claims Allowed	Validation	LOW	RESOLVED	p. 15
L-08	Deployment Order Warning	Warning	LOW	ACKNOWLEDGED	p. 16
L-09	Grayhat GLP Burn Warning	Warning	LOW	ACKNOWLEDGED	p. 17
L-10	Flash Close Prevented For Last Holder	Unexpected Behavior	LOW	ACKNOWLEDGED	p. 18

HIGH **H-01**

RESOLVED

Bad Debt Created By The Last Claimer

CATEGORY Gaming
 LOCATION MGLPV2Oracle.sol
 REVIEW Main Review

DESCRIPTION

The last claimer from the MagicGLP system can manipulate the oracle to report a higher price per share than is really available for the underlying MagicLP collateral shares.

This could be used to create bad debt as the final claimer who manipulates the price in this way can end up borrowing more MIM than their underlying shares are actually worth.

Consider the following example:

- Claimer A is the final claimer of tokens from the MagicLP upgraded contract
 - The totalSupply is 10e18 tokens
 - The total balance of the MagicLP contract is 10 GM tokens (assume GM is the only claim token for simplicity)
 - Claimer A claims all but 15 wei of their shares, e.g. `claim(10e18 - 15)`
 - Claimer A receives 99.9% of their claimed token amounts, leaving only some dust tokens in the vault
 - The price of Magic LP is consistent in this action
 - Now Claimer A maliciously sends `\$10` worth of GM tokens directly to the MagicLP contract
 - Notice that these funds are technically still under custody of Claimer A since they are the only holder of vault tokens
 - Now the state of MagicLP is, `totalSupply = 15 wei`, `TVL = \$10`
 - The MGLPV2Oracle reports the price as: `magicGlp.totalSupply() * 1e36 / (tv1 * 10**magicGlp.decimals()) => 15 * 1e36 / (10e18 * 1e18) = 1`
 - This is the inverse of price, measured as shares per asset. Therefore the value of shares reported by the oracle has been inflated due to the truncation.
 - With this price inflation the users 15 wei of collateral is valued at `\$15` in the CauldronV4 contract, meanwhile it can only be redeemed for `\$10` of TVL from the underlying vault
- This attack path could be scaled up with a bigger donation, allowing more MIM to be borrowed than can be recovered from the vault.

RECOMMENDATION

Consider rounding the resulting price up in the MGLPV2Oracle.

H-01 Bad Debt Created By The Last Claimer

CONTINUED

— RESOLUTION

Status: Resolved.

LOW **L-01**

RESOLVED

Zero Reward Claims DoS Claims

CATEGORY	DoS
LOCATION	MagicGlpRewardHandlerV2
REVIEW	Main Review

— DESCRIPTION

In the claim function when a token claim has zero value to be claimed the transfer is still attempted to the user. However for some ERC20 implementations a zero value transfer reverts.

This would DoS the claim action for users when a supported claim token has no balance in the contract or very small balance which rounds down to 0 during the claim calculations.

— RECOMMENDATION

Only perform the token transfer if the amount being transferred is nonzer.

— RESOLUTION

Status: Resolved.

LOW **L-02**

ACKNOWLEDGED

totalAssets Functions Unexpectedly

CATEGORY	Unexpected Behavior
LOCATION	MagicGLP, ERC4626
REVIEW	Main Review

— DESCRIPTION

The implementation of ERC4626 used by the MagicGLP contract relies on the `totalAssets` function to determine the result of the `convertToShares`, `convertToAssets`, `previewDeposit`, `previewMint`, `previewWithdraw`, `maxWithdraw`, and `previewRedeem` functions.

The RevertingToken contract is intended to disable the ERC4626 behavior, and the write functions from the ERC4626 contract have indeed been successfully disabled. However these view functions are not totally disabled and exhibit unexpected behavior because the `totalAssets` function does not revert.

The `totalAssets` function is intended to report how much underlying assets are available in the 4626 vault. And the `RevertingToken` has implemented the `balanceOf` function to allow `deal()` to be used in testing. As a result, rather than reverting, the `totalAssets` function returns an empty `balanceOf` result for the vault address. This results in unexpected results from the mentioned view functions, ranging from divide by zero panic reverts to successful executions with zero value results.

— RECOMMENDATION

Be aware of this unexpected behavior from these view functions and ensure that users do not rely on them to determine how much they can claim / redeem.

— RESOLUTION

Status: Acknowledged.

LOW **L-03**

RESOLVED

Callback Claim Tokens Exploit The System

CATEGORY	Callbacks
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

If a callback claim token is supported it can be leveraged to exploit the system because the attacker can gain control of the transaction after the shares have been burned but before subsequent claim token transfers have been processed in the claim function. This will result in a stepwise decrease in the price of the vault shares occurring after the malicious actors influence over the transaction passes, thus allowing them to open a loan at a higher exchange rate before it drops right afterwards.

— RECOMMENDATION

Be aware of this exploit for tokens with transfer callbacks and be sure to not support such tokens as claim tokens.

<unknown

url="https://app.notion.com/p/2468bda5828c80fe8251dc5d81c5b4aa#2428bda5828c80d38c7ffb3a9244acbb" alt="external_object_instance"/>

— RESOLUTION

Status: Resolved.

LOW **L-04**

ACKNOWLEDGED

Blacklisted Callee Safety Measure

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

No attack vector has been identified which uses the CALL action to call the underlying MagicLP vault contract directly from the Cauldron and before any solvency checks have been performed. However out of an abundance of caution, the MagicLP vault contract should be added as a blacklisted address.

— RECOMMENDATION

Blacklist the MagicLP vault contract for the MagicLP cauldron CALL action.

— RESOLUTION

Status: Acknowledged.

LOW **L-05**

ACKNOWLEDGED

Asset Edit Dangers

LOCATION Global

REVIEW Main Review

— DESCRIPTION

When adding or removing an asset there can be unexpected affects to the price of the vault shares. There will be a stepwise increase in the vault shares price if someone frontons the addition transaction and sends tokens to the vault, or they exist there already. And there will be a stepwise decrease in the vault shares if an asset is removed that includes a nonzero balance for the vault, this could cause some borrowing positions to go under water immediately.

— RECOMMENDATION

Be aware of these risks and ideally only configure assets before the system is live and do not edit them until all claims have been made.

— RESOLUTION

Status: Acknowledged.

LOW **L-06**

RESOLVED

GLP Yield Unclaimed

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

Any accumulated yield for the existing MagicLP system will be trapped after the upgrade.

— RECOMMENDATION

Consider claiming the current outstanding yield and understand that any yield which accumulates after the upgrade will have to be rescued.

— RESOLUTION

Status: Resolved.

LOW **L-07**

RESOLVED

0 Shares Claims Allowed

CATEGORY	Validation
LOCATION	MagicGlpUpgrade.sol
REVIEW	Main Review

— DESCRIPTION

The `claim` function performs no validation to ensure that the shares value provided is nonzero. As a result anyone can call the claim function even if they are not holders of `MagicGLP` and cause the `LogClaim` event to be emitted.

— RECOMMENDATION

Consider validating that the shares value provided is nonzero to avoid any unexpected execution paths or event emissions.

— RESOLUTION

Status: Resolved.

LOW **L-08**

ACKNOWLEDGED

Deployment Order Warning

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

Currently the `MagicGLP` cauldron is disabled because a reverting oracle is in place, however as soon as the `MGLPV20racle` is put in use the cauldron will become functional again.

If the MagicGLP upgrade is not completed before the cauldron is re-enabled, stepwise jumps in the value of MagicGLP shares may occur and cause unintended liquidations before all assets are tracked.

— RECOMMENDATION

Be sure that all redemption assets are sent to and are being tracked by the `MagicGLP` contract through the `MagicGlpRewardHandlerV2` implementation before the new Oracle is assigned to the Cauldron contract.

— RESOLUTION

Status: Acknowledged.

LOW **L-09**

ACKNOWLEDGED

Grayhat GLP Burn Warning

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

The GLP tokens held by the Grayhat are planned to be burned by the GMX team to effectively redistribute this amount to the rest of GLP holders.

This will cause a stepwise increase in the value of the MagicGLP shares as this value is appropriately re-distributed to GLP holders.

If the cauldron were to become re-activated before this burn takes place then users could be unfairly liquidated, as their GLP holdings (through MagicGLP) have not been updated in value.

— RECOMMENDATION

Consider waiting until the grayhat's GLP shares have been burned before setting the new non-reverting oracle implementation on the Cauldron.

— RESOLUTION

Status: Acknowledged.

LOW **L-10**

ACKNOWLEDGED

Flash Close Prevented For Last Holder

CATEGORY Unexpected Behavior

LOCATION Global

REVIEW Main Review

DESCRIPTION

The `MGLPV20racle` oracle reverts with a divide by zero revert when all shares of the vault have been redeemed and there is no TVL left in `MagicGLP`.

As a result, for the final claimer, if they happen to have a borrow position and attempt to use a flash-close method to withdraw their collateral and subsequently repay it, the solvency check at the end of the cook action will fail due to the oracle divide by zero revert.

RECOMMENDATION

Be aware of this quirk and consider returning zero as a result from the `MGLPV20racle` when the TVL amount is zero.

RESOLUTION

Status: Acknowledged.

§ 05

Disclaimer.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Guardian to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Guardian's position is that each company and individual are responsible for their own due diligence and continuous security. Guardian's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by Guardian is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis.

Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract's safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

§ 06

About Guardian.

Guardian is a smart contract security firm. Every engagement is worked by two independent teams competing on the same scope, each with its own tooling and methods, so no single reviewer's blind spot survives.

\$45B+DIGITAL ASSETS UNDER
REVIEW**200+**

ENGAGEMENTS COMPLETED

500+CRITICAL & HIGH FINDINGS
REPORTED

Reach us at audits@guardianaudits.com.