

GMX · SECURITY REVIEW

GMX

V2.3 Pre-Review.

A security review of V2.3 Pre-Review.

CLIENT	PROJECT	AUDITORS	AUDIT WINDOW	FINAL REPORT
GMX	V2.3 Pre-Review	Owen Thurm	July 24 – July 29, 2026	July 29, 2026

§ 00

Contents.

16 pages: overview, confidence ranking, scope, 7 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 · 7 findings	P. 07
§ 05	Disclaimer	P. 15
§ 06	About Guardian	P. 16

§ 01

Overview.

Guardian reviewed V2.3 Pre-Review across a single review round. The final report includes 7 Informational findings.

AUDIT FIRM	METHODOLOGY
Guardian	Smart contract · Manual · Main Review
CLIENT	
GMX	
PROJECT	
V2.3 Pre-Review	
PREPARED BY	
Owen Thurm	
AUDIT WINDOW	
July 24 – July 29, 2026	
FINAL REPORT	
July 29, 2026	

1.1 Confidence Ranking

5 / 5

Very High Confidence

Guardian assigns a Confidence Ranking of 5 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	0	0	0	0	0
Medium	0	0	0	0	0
Low	0	0	0	0	0
Informational	7	7	0	0	0
All severities	7	7	0	0	0

§ 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 ASSIGNED	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	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 V2.3 Pre-Review.

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					
I-01	Atomic account changes weaken order commitment	Business logic errors	INFORMATIONAL	PENDING	p. 7
I-02	Collateral caps can prevent isolated top-ups	Unexpected Behavior	INFORMATIONAL	PENDING	p. 9
I-03	Liquidation ignores aggregate close price impact	Logical Error	INFORMATIONAL	PENDING	p. 10
I-04	Atomic withdrawal lacks a non-atomic buffer	Oracle	INFORMATIONAL	PENDING	p. 11
I-05	Cross-margin withdrawal bypasses position check	Validation	INFORMATIONAL	PENDING	p. 12
I-06	PnL token whitelist removal breaks cross margin	Configuration	INFORMATIONAL	PENDING	p. 13
I-07	Swap paths bypass closed-market grace	Validation	INFORMATIONAL	PENDING	p. 14

INFORMATIONAL I-01

PENDING

Atomic account changes weaken order commitment

CATEGORY	Business logic errors
LOCATION	contracts/multichain/MultichainTransferRouter.sol; contracts/exchange/OrderHandler.sol
REVIEW	Main Review

— DESCRIPTION

The largest area of risk is the ability to atomically deposit to or withdraw from a cross-margin GMX Account in a single transaction while pending position actions execute later through the standard keeper/oracle path. This weakens the two-step commitment model used for position-level actions: instead of committing margin before execution pricing is known, a trader can change the margin backing the account after observing newer market information.

The concrete concern is increased exposure to short-term "risk-free trade" opportunities. If keeper execution uses a slightly stale but valid standard oracle price, a trader may be able to front-run execution by withdrawing collateral, or by deciding to deposit collateral only when required, in order to affect whether the pending action succeeds. A complete exploit normally also requires a trader-controlled condition that makes the keeper execution revert without cancelling or freezing the action for a period of time. No such non-frozen persistent failure path was identified in the reviewed normal order flow.

The risk may be accepted if keeper prices are expected to be maximally fresh. Even so, integrating the existing immediate multichain-balance deposit/withdrawal model with position collateral introduces this new effect and should be an explicit product and security decision.

— RECOMMENDATION

Clarify the product requirement for atomic cross-margin account deposits and withdrawals. If the feature is required, document the accepted oracle-freshness and selective-execution risk, and add adversarial tests covering atomic account-balance mutations immediately before all relevant keeper actions. Otherwise, consider restoring a commitment boundary by locking relevant account collateral while actions are pending or by requiring a compatible price-freshness regime for account changes and keeper execution.

I-01 Atomic account changes weaken order commitment

CONTINUED

— **RESOLUTION**

Status: Pending.

INFORMATIONAL I-02

PENDING

Collateral caps can prevent isolated top-ups

CATEGORY	Unexpected Behavior
LOCATION	contracts/market/CrossCollateralUtils.sol; contracts/position/IncreasePositionUtils.sol
REVIEW	Main Review

DESCRIPTION

An isolated position has exactly one collateral token. If that token is cross collateral and its market-level cap is exhausted, the user cannot add collateral to improve the position's health using another token. Unlike cross margin, isolated positions cannot fall back to another eligible token. This can leave users unable to restore a position's safety margin except by reducing or closing it.

RECOMMENDATION

Explicitly document this cap-induced top-up limitation and assess whether an isolated collateral migration or conversion mechanism is needed. Ensure UX and liquidation behavior make the risk clear.

RESOLUTION

Status: Pending.

INFORMATIONAL I-03

PENDING

Liquidation ignores aggregate close price impact

CATEGORY	Logical Error
LOCATION	contracts/position/CrossMarginAccountUtils.sol; contracts/position/CrossMarginLiquidationUtils.sol
REVIEW	Main Review

— DESCRIPTION

Cross-margin liquidation eligibility aggregates marked collateral, recognized PnL, accrued fees, and maintenance requirements. It does not simulate the execution price impact of closing all account positions, including interactions among positions that share a virtual inventory. An account may appear adequately margined at mark price even though the sequence of required liquidation closes realizes materially worse outcomes.

— RECOMMENDATION

Model conservative close price impact in account health, or add a calibrated liquidation buffer that covers correlated position unwinds and shared virtual-inventory effects. Validate the chosen model with multi-position same-market scenarios.

— RESOLUTION

Status: Pending.

INFORMATIONAL I-04

PENDING

Atomic withdrawal lacks a non-atomic buffer

CATEGORY	Oracle
LOCATION	contracts/multichain/MultichainTransferRouter.sol; contracts/oracle/Oracle.sol
REVIEW	Main Review

— DESCRIPTION

transferOutWithOraclePrices permits an immediate account withdrawal after checking health using atomic oracle prices. No additional buffer is applied to protect the account against valuation under the standard non-atomic execution oracle. An account can pass the fresh atomic health check while becoming liquidatable or materially weaker when evaluated by the standard price provider used by later keeper actions.

— RECOMMENDATION

Apply a conservative buffer or dual-price health validation to atomic withdrawals, or require the post-withdrawal account to remain safe under a valuation compatible with subsequent standard-oracle actions.

— RESOLUTION

Status: Pending.

INFORMATIONAL I-05

PENDING

Cross-margin withdrawal bypasses position check

CATEGORY	Validation
LOCATION	contracts/multichain/MultichainTransferRouter.sol; contracts/position/IncreasePositionPostUtils.sol; contracts/position/DecreasePositionValidationUtils.sol
REVIEW	Main Review

DESCRIPTION

An oracle-priced withdrawal from the GMX account validates only aggregate cross-margin account liquidation state. It does not apply the isolated willPositionCollateralBeSufficient safeguard, which excludes positive PnL and enforces a position-local dynamic collateral requirement intended to resist price-impact manipulation. Cross-margin users can therefore withdraw through a path that does not reproduce those per-position protections.

RECOMMENDATION

Document and justify the intentional replacement of the position-local safeguard, or apply an equivalent conservative per-position constraint to account withdrawals. At minimum, assess whether the aggregate test must exclude positive PnL or model the same dynamic collateral requirement.

RESOLUTION

Status: Pending.

INFORMATIONAL I-06

PENDING

PnL token whitelist removal breaks cross margin

CATEGORY	Configuration
LOCATION	contracts/config/ConfigOperationalUtils.sol; contracts/config/Config.sol
REVIEW	Main Review

— DESCRIPTION

Enabling a market for cross margin validates that both possible PnL payout tokens are whitelisted and configured. Removing a collateral token from the whitelist only checks active cross-collateral usage for that token. It does not check whether the token remains a possible PnL token for an enabled cross-margin market, and does not disable affected markets or require their positions to close. Governance can therefore leave an enabled market and open cross-margin positions in a state that violates the prerequisite used when cross margin was enabled.

— RECOMMENDATION

Block removal of a whitelisted token while it is a long or short PnL token for any cross-margin-enabled market, or atomically disable all affected markets and require positions to be closed or migrated before removal.

— RESOLUTION

Status: Pending.

INFORMATIONAL **I-07**

PENDING

Swap paths bypass closed-market grace

CATEGORY	Validation
LOCATION	contracts/exchange/OrderHandler.sol; contracts/market/MarketUtils.sol
REVIEW	Main Review

— DESCRIPTION

Collateral-only MarketIncrease orders bypass the closed-market grace checks when sizeDeltaUsd is zero. The exception does not require an empty swap path. A user can therefore execute a zero-size increase that swaps through one or more path markets while the grace-period protections are bypassed. More generally, order swap-path validation checks markets are enabled but does not apply the path markets' closed-state, grace-period, feature-gate, or price-consistency validation.

— RECOMMENDATION

In swaps validate every path market's closed-state, grace period, feature gate, and price consistency during execution.

— RESOLUTION

Status: Pending.

§ 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.