

GMX · SECURITY REVIEW

GMX

Open Interest Updates Plan.

A security review of Open Interest Updates Plan.

CLIENT	PROJECT	AUDITORS	AUDIT WINDOW	FINAL REPORT
GMX	Open Interest Updates Plan	Guardian	December 14 – December 20, 2025	December 20, 2025

§ 00

Contents.

16 pages: overview, confidence ranking, scope, 5 findings, disclaimer, and about Guardian.

§ 01	Overview	P. 03
§ 02	Confidence Ranking	P. 04
§ 03	Scope & Classifications	P. 05
	Files in Scope	P. 06
§ 04	Findings	P. 07
	Main Review · 5 findings	P. 08
§ 05	Disclaimer	P. 15
§ 06	About Guardian	P. 16

§ 01

Overview.

Guardian reviewed Open Interest Updates Plan across 2 review rounds. The final report includes 1 High, 1 Medium, 3 Low findings.

AUDIT FIRM	REPOSITORY
Guardian	https://github.com/gmx-io/gmx-synthetics
CLIENT	METHODOLOGY
GMX	Smart contract · Manual · Main Review · Remediation Review
PROJECT	MAIN REVIEW COMMIT
Open Interest Updates Plan	6cc69866b5e5
PREPARED BY	REMEDATION REVIEW COMMIT
Guardian	a0894ab321cf
AUDIT WINDOW	
December 14 – December 20, 2025	
FINAL REPORT	
December 20, 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	1	0	0	1	0
● Low	3	0	3	0	0
● Informational	0	0	0	0	0
All severities	5	0	3	1	1

§ 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 Open Interest Updates Plan in <https://github.com/gmx-io/gmx-synthetics>. The scope includes 275 source lines across 1 file.

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.

Files in Scope.

FILE	NSLOC	TOTAL
MAIN REVIEW		
scripts/syncVirtualPriceImpact.ts	130	156
REMEDIATION REVIEW		
scripts/syncVirtualPriceImpact.ts	145	170

§ 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	Homogenous Markets Double Count OI	Logical Error	HIGH	RESOLVED	p. 8
M-01	De-sync Risk At Step 5	Warning	MEDIUM	PARTIALLY RESOLVED	p. 10
L-01	De-sync Risk Between Steps 2 and 3	Warning	LOW	ACKNOWLEDGED	p. 11
L-02	Simulation Gaps	Warning	LOW	ACKNOWLEDGED	p. 13
L-03	Orders May Fail And Allow Stepwise Jumps	Warning	LOW	ACKNOWLEDGED	p. 14

HIGH **H-01**

RESOLVED

Homogenous Markets Double Count OI

CATEGORY Logical Error

LOCATION Global

REVIEW Main Review

DESCRIPTION

Throughout the `syncVirtualPriceImpact` script as well as the simulation scripts the open interest in tokens from markets that have homogenous backing tokens is double counted, as the scripts always assume that the backing collateral tokens don't point to the same storage key slot in the `dataStore`.

This can be observed by the output of the simulation scripts, the output for tBTC is as follows:

```
``markdown
```

11	'BTC tBTC-tBTC'	'0xd6206869...'	'678687328'	'639758694'	'\$606498 / \$598881'
'\$574195 / \$564530'	'Longs / Longs'	'4.733089e-8 / 4.733089e-8'	'+0.00%'	'0.000000e+0 /	
0.000000e+0'	'0.00%'	'1.518152e-8 / 1.518152e-8'	'+0.00%'	'Longs / Longs'	'\$33.14 /
\$33.14'	'+\$0.00 (+0.00%)'	'-\$547.36 / -\$753.65'	'+37.68% / -\$206.29'	'-\$13644.79 /	
-\$240.45'	'-98.23% / +\$13404.33'				

```
``
```

Claiming that the long OI is 678687328 in tokens, however the corresponding key in the `dataStore` only shows half of that:

This will perturb every virtual inventory that includes a market with homogenous backing tokens.

RECOMMENDATION

A divisor check and application for homogenous markets would be the most straightforward fix, as is done in the contracts. However we should avoid dividing by 2 to create any rounding errors unnecessarily. Instead, for homogenous markets simply only query the key once for the long side and the short side, with the knowledge that the collateral tokens are the same.

H-01 Homogenous Markets Double Count OI

CONTINUED

— RESOLUTION

Status: Resolved.

MEDIUM **M-01**

PARTIALLY RESOLVED

De-sync Risk At Step 5

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

The `syncVirtualPriceImpact.ts` script is intended to read the net size in tokens across all markets in a virtual inventory group and the pass that result to be synced onchain through the `Config`. However the time at which the values for the size in tokens are read and the time at which the configuration is synced onchain are at two different times, and may have blocks recorded on the Arbitrum network in-between them.

The time at which the script records the size in tokens across markets in a group is at script execution time. The time at which the configurations are synced is at the time of the block which ultimately ends up including the configuration transaction.

If any action which updates the size in tokens in any market within that group occurs in a block between those two times, then this will cause a desync between the value stored in the virtual inventory and the value of size in tokens actually within the markets inside the virtual group.

— RECOMMENDATION

Consider adding an additional step, which is a script that checks the values in the virtual inventory for tokens and compares it with the actual aggregate size in tokens of the markets in the group to ensure that no desync has occurred. If one has occurred then another configuration can be made specifically for that market which probabilistically will not have the same issue.

— RESOLUTION

Status: Partially resolved.

LOW **L-01**

ACKNOWLEDGED

De-sync Risk Between Steps 2 and 3

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

— DESCRIPTION

The virtual inventory script is meant to sync the current net long or net short exposure in tokens to the new virtual inventory in tokens.

The plan steps are as follows:

```
```markdown
```

1. run script to create long and short positions for all markets
  2. run script to sync virtual inventory
  3. turn on flag
  4. re-run script to create long and short positions for all markets
  5. re-run script to sync virtual inventory
- ```
```
```

The contracts will not begin to track updates to the virtual inventory in tokens until the flag is switched. Therefore if anyone performs an action between steps 2 and 3 that would change the `sizeInTokens` of any position in any market then it will cause a desync between the value stored in the virtual inventory in tokens and the actual market value.

In step 5 there is a re-sync of the virtual inventory which should correct any de-sync that could have happened. However it may be the case that in the event of a de-sync after step 2 that the price impact results from the virtual inventory can be wrong and there could be unexpected reverts that occur as a result of the virtual inventory being de-synced. This may interfere with the completion of step 4.

### — RECOMMENDATION

Be aware of this risk when executing the scripts. Consider turning off access to actions through the UI during the migration, or halting keepers from execution position actions / pausing markets to totally remove the possibility of a desync.

---

**L-01** De-sync Risk Between Steps 2 and 3

CONTINUED

---

— **RESOLUTION**

Status: Acknowledged.

LOW **L-02**

ACKNOWLEDGED

## Simulation Gaps

CATEGORY	Warning
LOCATION	Global
REVIEW	Main Review

### — DESCRIPTION

The simulation script does not use exactly the script that will be executed in the actual migration, the `syncVirtualPriceImpact` script, to do its syncing simulation. This could create a gap between the simulation and the actual migration.

### — RECOMMENDATION

Consider re-running the simulation adapting it for the actual `syncVirtualPriceImpact` script which will be run.

### — RESOLUTION

Status: Acknowledged.

LOW **L-03**

ACKNOWLEDGED

## Orders May Fail And Allow Stepwise Jumps

CATEGORY Warning  
LOCATION Global  
REVIEW Main Review

### — DESCRIPTION

At steps 1 and 4 it may be possible that the orders created fail in some markets due to market conditions, validations, or gas issues.

### — RECOMMENDATION

Be aware of this possibility and ensure that all orders are successfully executed before moving on to the next step.

### — 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](mailto:audits@guardianaudits.com).