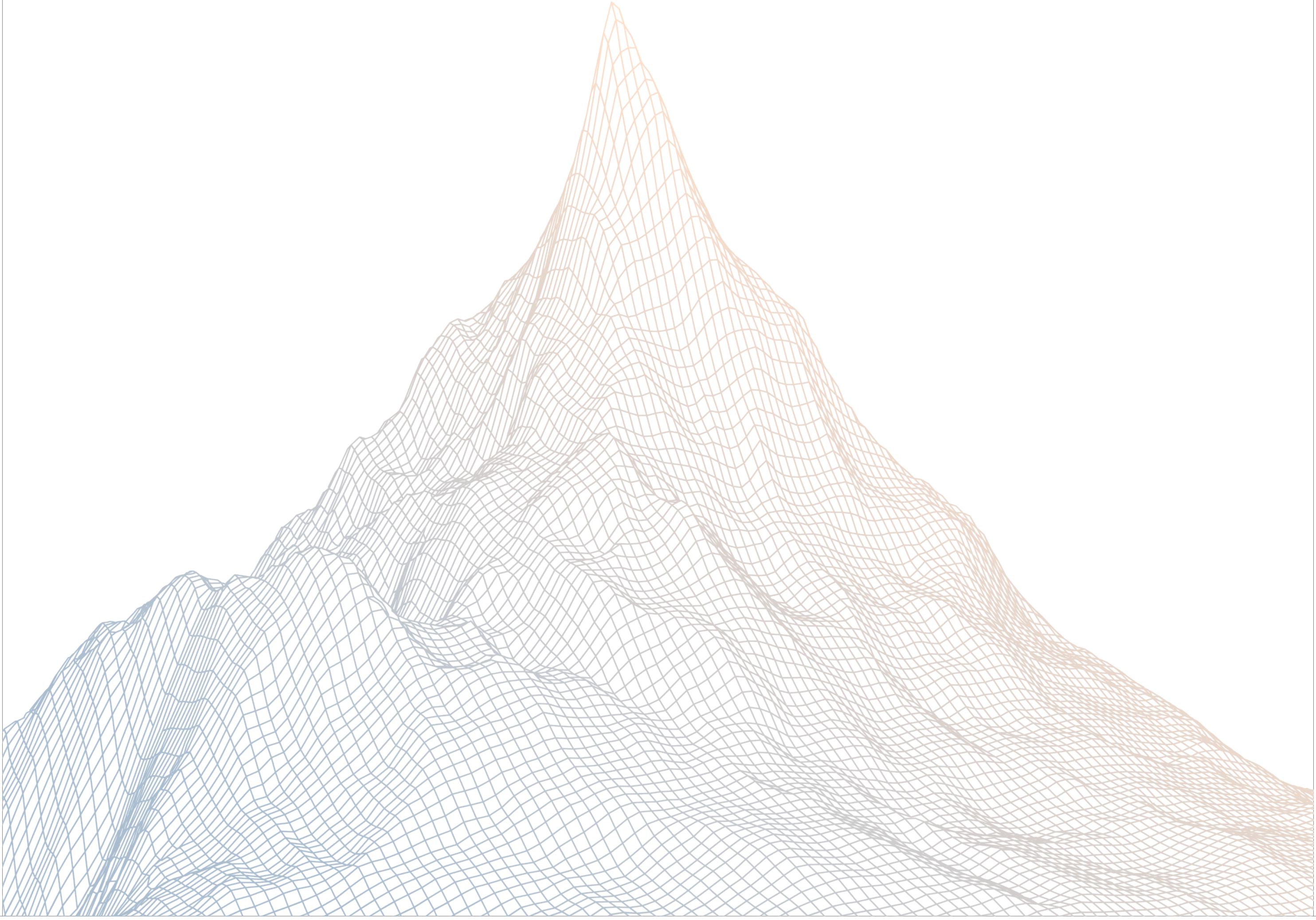
Zenith

GMX Solana

Smart Contract Security Assessment

VERSION 1.1



AUDIT DATES:	August 8th to August 8th, 2025
AUDITED BY:	DadeKuma IIIIIII000 peakbolt

Contents

1 Introduction

1.1 About Zenith

Zenith assembles auditors with proven track records: finding critical vulnerabilities in public audit competitions.

Our audits are carried out by a curated team of the industry's top-performing security researchers, selected for your specific codebase, security needs, and budget.

Learn more about us at https://zenith.security.

1.2 Disclaimer

This report reflects an analysis conducted within a defined scope and time frame, based on provided materials and documentation. It does not encompass all possible vulnerabilities and should not be considered exhaustive.

The review and accompanying report are presented on an "as-is" and "as-available" basis, without any express or implied warranties.

Furthermore, this report neither endorses any specific project or team nor assures the complete security of the project.

1.3 Risk Classification

SEVERITY LEVEL	IMPACT: HIGH	IMPACT: MEDIUM	IMPACT: LOW
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

2

Executive Summary

2.1 About GMX Solana Protocol

GMX Solana is a decentralized spot and perpetual exchange that supports low swap fees and low price impact trades.

Trading is supported by unique multi-asset pools that earns liquidity providers fees from market making, swap fees and leverage trading.

Dynamic pricing is supported by Chainlink Oracles and an aggregate of prices from leading volume exchanges.

2.2 Scope

The engagement involved a review of the following targets:

Target	gmx-solana
Repository	https://github.com/gmsol-labs/gmx-solana/
Commit Hash	`f6d3de65367c4bff6ee5539e89dc82aa077cf75f`
Files	`Changes in PR-146`

Target	GMX Solana Mitigation Review
Repository	https://github.com/gmsol-labs/gmx-solana
Commit Hash	`cd0dfc84b5e2b1857f54c6cdbe25459fb6e43145`
Files	`Changes in the latest source code version`

2.3 Audit Timeline

August 8, 2025	Audit start
August 8, 2025	Audit end
August 14, 2025	Report published

2.4 Issues Found

SEVERITY	COUNT
Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	2
Informational	2
Total Issues	**4**

3

Findings Summary

ID	Description	Status
L-1	Large RWA trades can sometimes be made without affecting the oracle's price	Acknowledged
L-2	Inconsistent field names between V2 and V7 report schemas	Resolved
I-1	LastUpdateDiffSecs flag should not be set for non-V8 reports	Resolved
I-2	Typos	Resolved

4 Findings

4.1 Low Risk

A total of 2 low risk findings were identified.

[L-1] Large RWA trades can sometimes be made without affecting the oracle's price

SEVERITY: Low	IMPACT: Low
STATUS: Acknowledged	LIKELIHOOD: Low

Target

- crates/chainlink-datastreams/src/gmsol.rs
- crates/model/src/pool/delta.rs
- crates/programs/src/model/market.rs

Description:

The Chainlink data streams documentation says the following about the `market_status` field it provides:

> The market status provided on Streams serves as an indication of the open and close hours for traditional market assets based on historical practice; it is provided for referential purposes only. Developers are responsible for independently assessing the risks associated with trading at these times, particularly at opening and closing price levels. Developers are solely responsible for determining the actual status of markets for any streams they utilize.

This means that, for example, for NYSE/NASDAQ securities, the market is considered as open at 9:30am and is considered closed at 4:00pm. The market's liquidity usually mirrors these bounds, but there are some cases where it does not. For example, if there was an earnings announcement while the market was closed and this announcement resulted in a large price gap, the market's actual opening cross trade may happen anywhere between a few seconds to a few minutes after 9:30am. During this delay there is extremely low liquidity, and often times when the opening cross trade prints, there is a not-insignificant price gap between the price just before the cross, and the crossing price.

Since the indicated opening cross price is published every second (out of band), an attacker can submit a large market-on-open order on a CEX for a security where there is currently a gap between the indicated open, and the NBBO price quoted by the Chainlink data stream, and enter the closing trade on the gmsol DEX using the low-liquidity price, locking in an immediate profit. The purpose of price impact is to add a sort of rate limiting in order to prevent market manipulation, but gmsol only has one setting for price impact, so the trader will be able to fill using the price impact that is available during normal trading, rather than an increased impact for this low-liquidity period.

A similar issue exists during market halts, where there is actually _zero_ liquidity available on a CEX. Once the reason for the halt is made known, it is usually straight forward to determine in which direction the price will gap when it re-opens. An attacker can wait until it's known, then open the opposite position on the gmsol DEX in size, then exit on the CEX when the halt ends. The change to track last-update-diffs in seconds in order to allow for the case where the bid/ask hasn't changed for a few minutes, implies that the heartbeat will now be at least on the order of seconds, which will make the halt issue much more likely to be exploitable.

Recommendations:

For the market open issue, a mitigation could be to have massively increased price impacts for the first hour of trading of a market. For the trading halts issue, it is not possible to completely resolve this issue without requiring that every gmsol trade occur during the same second as the `last_update_timestamp`, but this would cause the code to continue to unfairly prevent traders from closing their positions when there hasn't been a bid/ask change in a while (e.g. just prior to market close, which would cause them to incur overnight risk). A preferable change for solving both would be having Chainlink introduce more rigorous tracking of trading halts and market open/close, and open/close/halt epochs, so that the distance between the `last_update_timestamp` and `observations_update` doesn't have to be used to infer whether the price is still valid.

GMX: Acknowledged. Let me summarize our thoughts:

1. We believe that only risk-free or extremely low-risk arbitrage **within the protocol** constitutes an attack (thereby causing ongoing losses to LPs). Using the protocol to conduct arbitrage **outside** the protocol is considered normal trading activity and can even be beneficial to the protocol.

2. We agree that the information provided in Chainlink reports is insufficient to fully address issues arising from market halts. Based solely on the `last update timestamp`, it is difficult to accurately determine whether the market is truly halted or simply experiencing a temporary lack of trades. If the market is indeed halted but the protocol still treats it as open, traders with more information could potentially open positions in the protocol ahead of others to gain an advantage. However, this still may not qualify as risk-free arbitrage, since in theory such traders cannot be certain whether the post-reopen price will necessarily be in their favor.

In the future, we plan to introduce temporary increases to min collateral factor and borrowing fees during market halts in the next version, helping LPs hedge against the risks of such behavior. Additionally, keepers will be allowed to liquidate positions that fall below the temporary collateral factor during the halt. Therefore, for now, we can log this issue as a **known issue**.

3. For the delayed market open scenario you mentioned, we can assume that the time window during which external exchanges have low liquidity is sufficiently long (otherwise the time adjustment delayed-execution mechanism alone would be enough to mitigate the attack risk).

If the price impact parameter is set appropriately, an attacker's opening and closing of positions within the protocol would incur a significant price impact cost (because, for manipulation to be profitable, the position size within the protocol must be large enough), making such an attack unprofitable.

The appropriateness of the price impact parameter is ensured by the risk parameter provider, and such parameter updates can be made promptly. The already-deployed off-chain Risk Oracle system monitors the liquidity conditions of external markets to assess the profitability of price manipulation and automatically updates the price impact parameter. If there is no Risk Oracle system, the risk parameters can instead be set to a more conservative level such that even under low external liquidity conditions, manipulation remains unprofitable.

That said, we believe it's still necessary to respond to the points you raised:

- Price impact is primarily intended to prevent manipulation of oracle prices for profit by exploiting liquidity differences. The price impact parameter is adjusted in real time based on liquidity in external exchanges, but its primary purpose remains making such manipulation unprofitable.
- Even if the market status is indicated as open, temporary halts will still be detected based on the last update timestamp and trading will be blocked once the threshold is exceeded.
- The main reason trading is prohibited during market halts is that prices no longer reflect market information during these periods. This would allow traders to use deterministic information to conduct low-risk or even risk-free arbitrage within the protocol — for example, opening positions during the halt and closing them after the market reopens with a price gap.

Zenith: Given that there isn't a known attack vector for the halt scenario that involves extremely low-risk arbitrage from within the protocol, but it is possible enough that one exists that the protocol plans to implement safeguards just in case, the market halts aspect of the finding is low-risk. Given that there is already an off-chain mitigation for the potential low liquidity after market open, the risk there is low too. Therefore, we've downgraded the severity of this finding to Low.

[L-2] Inconsistent field names between V2 and V7 report schemas

`SEVERITY`: Low	`IMPACT`: Informational
`STATUS`: Resolved	`LIKELIHOOD`: Low

Target

- crates/chainlink-datastreams/src/report.rs

Description:

The protocol currently uses the same decoding logic for both V2 and V7 datastream reports, despite their naming differences (V2 uses `benchmark_price` while V7 uses `exchange_rate`).

While technically functional since both fields share the same data type, this implementation could create confusion, as the field naming discrepancy isn't properly documented.

Recommendations:

Consider implement version-specific decoding logic that properly handles both V2 and V7 report formats.

GMX Solana: Resolved with @ad0c4e88f7...

Zenith: Verified.

4.2 Informational

A total of 2 informational findings were identified.

[I-1] `LastUpdateDiffSecs` flag should not be set for non-V8 reports

`SEVERITY:` Informational	`IMPACT:` Informational
`STATUS:` Resolved	`LIKELIHOOD:` Low

Target

- crates/chainlink-datastreams/src/gmsol.rs
- crates/chainlink-datastreams/src/report.rs
- crates/utils/src/price/mod.rs

Description:

The `PriceFlag::LastUpdateDiffSecs` is unconditionally set to `true` for all Chainlink data-streams updates, since after the upgrade only seconds are used for new values. However, when there is no `last_update_timestamp` field, it's nonsensical for a field that does not exist (e.g. in a V3 `Report`) to be "in seconds".

Recommendations:

Only set the secs flag if the enabled flag is set:

```
 price.set_flag(PriceFlag::Open, is_open);
price.set_flag(
    PriceFlag::LastUpdateDiffEnabled,
    last_update_diff_secs.is_some(),
);
price.set_flag(PriceFlag::LastUpdateDiffSecs, true);
if last_update_diff_secs.is_some() {
    price.set_flag(PriceFlag::LastUpdateDiffEnabled, true);
    price.set_flag(PriceFlag::LastUpdateDiffSecs, true);
}
```

GMX Solana: Resolved with @a7e1f77ae9...

Zenith: Verified

[I-2] Typos

SEVERITY: Informational	IMPACT: Informational
STATUS: Resolved	LIKELIHOOD: Low

Target

- crates/chainlink-datastreams/src/gmsol.rs

Description:

The following typos were identified:

`treasted -> treated`

```
// treasted as the market being closed.
```

Recommendations:

We recommend fixing the typo.

GMX Solana: Resolved with @a6e83147fc...

Zenith: Verified.