GUARDIAN AUDITS

SMART CONTRACT SECURITY AUDIT OF

GMX

Summary

Audit Firm Guardian

Prepared By Owen Thurm, Daniel Gelfand

Client Firm GMX

Final Report Date November 26, 2023

Audit Summary

GMX engaged Guardian to review the security of its subaccount updates. From the 30th of October to the 5th of November, a team of 2 auditors reviewed the source code in scope. All findings have been recorded in the following report.

Notice that the examined smart contracts are not resistant to internal exploit. For a detailed understanding of risk severity, source code vulnerability, and potential attack vectors, refer to the complete audit report below.

🔗 Blockchain network: **Arbitrum**

✅ Verify the authenticity of this report on Guardian's GitHub: https://github.com/guardianaudits

Table of Contents

Project Overview

Project Summary

Project Name	GMX
Language	Solidity
Codebase	https://github.com/gmx-io/gmx-synthetics
Commit(s)	Initial: f620b30e5c9bd8a1b0cdb3532d706218a05cf672 Final: 79b216674873dd7cebcea3ce3e7405b164059241

Audit Summary

Delivery Date	November 26, 2023
Audit Methodology	Static Analysis, Manual Review

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	1	0	0	0	0	1
Low	5	o	0	3	0	2

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
SUBR	SubaccountRouter.sol	6177e187773722e807e67e10d520c9e32e9b811d
SUBU	SubaccountUtils.sol	3e55bfc94d9fa8b512b4b6bb2329b3fa40d43346
BRTE	BaseRouter.sol	38544eb7a3b0155f6c036c0ad4e45dc1642d0a1b

Audit Scope & Methodology

Vulnerability Classifications

Vulnerability Level	Classification
🔴 Critical	Easily exploitable by anyone, causing loss/manipulation of assets or data.
🟠 High	Arduously exploitable by a subset of addresses, causing loss/manipulation of assets or data.
🟡 Medium	Inherent risk of future exploits that may or may not impact the smart contract execution.
🟢 Low	Minor deviation from best practices.

Methodology

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.
- Comprehensive written tests as a part of a code coverage testing suite.
- Contract fuzzing for increased attack resilience.

Findings & Resolutions

ID	Title	Category	Severity	Status
SUBR-1	Unnecessary Top Up	Logical Error	Medium	Resolved
SUBR-2	Inconsistent address(0) Checks	Validation	Low	Resolved
SUBU-1	Add And Remove Subaccount Events Always Emitted	Events	Low	Acknowledged
SUBU-2	Mission actionType Field In Events	Events	Low	Resolved
GLOBAL-1	Subaccount Risk	Warning	Low	Acknowledged
SUBR-3	Passed Address Not Necessarily A Subaccount	Validation	Low	Acknowledged

SUBR-1 | Unnecessary Top Up

Category	Severity	Location	Status
Logical Error	Medium	SubaccountRouter.sol: 140	Resolved

Description

In the `_handleSubaccountAction` function, the subaccount is always topped up by the `autoTopUpAmount` however this fixed top up amount is applied even when the subaccount did not cover any `executionFee`.

For example, a subaccount may cancel an order and be topped up, however no `executionFee` was necessary to perform the cancellation. Similarly, a subaccount may update an order and the update may require little or no additional `executionFee`, yet the same fixed top up amount will be sent to the subaccount.

Additionally, certain order types require more `executionFee` than others, currently a fixed `autoTopUpAmount` cannot perfectly remunerate for any type of order.

Recommendation

Consider only topping up the subaccount if an order was created or an update was made that required a non-trivial amount of `executionFee`.

Additionally, consider fluctuating the `autoTopUpAmount` depending on the type of order created as the `executionFee` required may vary significantly, though a configurable fixed `autoTopUpAmount` may be fine.

Resolution

GMX Team: The recommendation was implemented in commit 2349c80.

SUBR-2 | Inconsistent address(0) Checks

Category	Severity	Location	Status
Validation	Low	SubaccountRouter.sol: 110	Resolved

Description

In the `cancelOrder` function there is validation that the `order.account()` is not the zero address, however this validation is not present in the `updateOrder` function which similarly accesses an order from an arbitrary key provided by the caller.

Recommendation

Consider adding validation in the `updateOrder` function such that the `order.account()` cannot be the zero address to match the validation present in the `cancelOrder` function.

Resolution

GMX Team: The recommendation was implemented in commit 2349c80.

SUBU-1 | Add And Remove Subaccount Events Always Emitted

Category	Severity	Location	Status
Events	Low	SubaccountUtils.sol: 19, 42	Acknowledged

Description

The `addSubaccount` and `removeSubaccount` functions emit the `AddSubaccount` and `RemoveSubaccount` events regardless of whether the subaccount was actually added to the subaccount set or actually removed from the subaccount set.

Therefore a subaccount address may be removed from a `subaccountList` where the subaccount is not present, or added to one where the subaccount is already present in order to manipulate systems relying on the `AddSubaccount` and `RemoveSubaccount` events.

Recommendation

Consider only emitting the `AddSubaccount` and `RemoveSubaccount` events if the subaccount was actually added or removed from the subaccount set.

Resolution

GMX Team: Acknowledged.

SUBU-2 | Mission actionType Field In Events

Category	Severity	Location	Status
Events	Low	SubaccountUtils.sol: 65, 93	Resolved

Description

In the `incrementSubaccountActionCount` function, the `IncrementSubaccountActionCount` event emitted lacks the `actionType` as a field. This is crucial information to differentiate actions for any systems relying on the `IncrementSubaccountActionCount` event.

Similarly in the `setMaxAllowedSubaccountActionCount` function, the `SetMaxAllowedSubaccountActionCount` event lacks the `actionType`.

Recommendation

Consider including the `actionType` as a field for the `IncrementSubaccountActionCount` and `SetMaxAllowedSubaccountActionCount` events.

Resolution

GMX Team: The recommendation was implemented in commit 2349c80.

GLOBAL-1 | Subaccount Risk

Category	Severity	Location	Status
Warning	Low	Global	Acknowledged

Description

Subaccounts for users must always be trusted as they can create arbitrary orders for a user's position, potentially forcing their position closer to liquidation.

Additionally, subaccounts can update and cancel orders created by the user or even other subaccounts.

Recommendation

Be sure to document this risk for users who wish to use the subaccount feature.

Resolution

GMX Team: Acknowledged.

SUBR-3 | Passed Address Not Necessarily A Subaccount

Category	Severity	Location	Status
Validation	Low	SubaccountRouter.sol: 48, 65	Acknowledged

Description

In both functions `setMaxAllowedSubaccountActionCount` and `setSubaccountAutoTopUpAmount`, the passed `address subaccount` may not actually be a subaccount of the account, but the state will be updated regardless, and the events will still emit.

Recommendation

If this behavior is unintended, add a call to `validateSubaccount` prior to updating the Datastore.

Resolution

GMX Team: Acknowledged.

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.

About Guardian Audits

Founded in 2022 by DeFi experts, Guardian Audits is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian Audits upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit https://guardianaudits.com

To view our audit portfolio, visit https://github.com/guardianaudits

To book an audit, message https://t.me/guardianaudits