GUARDIAN AUDITS

SMART CONTRACT SECURITY AUDIT OF

GMX

Summary

Audit Firm Guardian

Prepared By Owen Thurm, Daniel Gelfand

Client Firm GMX

Final Report Date September 26, 2023

Audit Summary

GMX engaged Guardian to review the security of its adaptive funding fee remediations. From the 18th of September to the 25th of September, 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, Avalanche**

✅ 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)	85cee2f67c7d01c893122a6baf52fdb6bfef7916

Audit Summary

Delivery Date	September 26, 2023
Audit Methodology	Static Analysis, Manual Review, Contract Fuzzing

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	0	0	0	0	0	0
Low	3	3	0	0	0	0

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
CON	Config.sol	c96b43934a499e54fd9b7e10f91b6d89d2d5eebb
KEY	Keys.sol	8d22e0946dd42d1c9292482f56d288d4db4dcc58
EDPU	ExecuteDepositUtils.sol	4dc96caf9adc0a3d4ec270bc5bfcff699a99b0e3
BOH	BaseOrderHandler.sol	bad36e5a42a06bd158c14ae478e875caae58c480
GSU	GasUtils.sol	965abfc84662baf289cba50424d9f6b7effaf89c
MKTU	MarketUtils.sol	c20a07e4e8a0a28223662f4aa6dccb7dae72abf8
OCL	Oracle.sol	e238cbd38f9a8daa9df6caf2685d6877f3c9b52f
PSU	PositionUtils.sol	383174bdb57860b999a5d9a85dcf9f6894cbeb05
BRTR	BaseRouter.sol	38544eb7a3b0155f6c036c0ad4e45dc1642d0a1b
ERTR	ExchangeRouter.sol	09d06d9870acbc23180755cb4588f9296d7663bc
TKU	TokenUtils.sol	2569b611038b1951c2fca4d407bbd4d832877007
CALC	Calc.sol	762c6d23b64c1d2f3ea4d8ba9ca7926dac90d83e
EWDU	ExecuteWithdrawalUtils.sol	85f61f75ec9ce9f940cf5ab0d356827ce93336c0

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.

Invariants Assessed

During Guardian's review of the GMX V2 system updates, fuzz-testing with Foundry was performed on a key function.

Throughout the engagement the following invariant was assessed for a total of 2,000,000+ runs with a prepared Foundry fuzzing suite.

ID	Description	Definition	Run Count
CALC-1	boundMagnitude successfully bounds the magnitude of the resulting value between the min and max	min <= boundMagnitude(value, min, max).abs() <= max	2,000,000+

Findings & Resolutions

ID	Title	Category	Severity	Status
CALC-1	boundMagnitude Exceeds Int256 Range	Documentation	Low	Pending
BRTR-1	Redundant Validation	Superfluous Code	Low	Pending
BRTR-2	Missing Documentation	Documentation	Low	Pending

CALC-1 | boundMagnitude Exceeds Int256 Range

Category	Severity	Location	Status
Documentation	Low	Calc.sol: 28-30	Pending

Description

In the `Calc.boundMagnitude` function, it is possible for the type casting to exceed the value range for an `int256`, producing a revert with the `SafeCast` library.

If the `value` parameter is the minimum `int256` value, the bounding will fail with a `SafeCast` revert as the absolute value will not fit in an `int256` type.

Furthermore, if the `min` is greater than `type(int256).max`, the resulting `magnitude` will exceed `type(int256).max` which results in a `SafeCast` revert when casting `toInt256()`.

Recommendation

Though currently this case will likely never be possible, consider documenting that the function will fail when `value=type(int256).min` and when the `min` bound is outside of the range of values for `int256` type.

Resolution

BRTR-1 | Redundant Validation

Category	Severity	Location	Status
Superfluous Code	Low	BaseRouter.sol: 38, 50	Pending

Description

The `validateReceiver` validations in the `sendNativeToken` and `sendWnt` functions are superfluous as the `receiver` is immediately validated in the `TokenUtils.sendNativeToken` and `TokenUtils.depositAndSendWrappedNativeToken` functions.

Recommendation

Remove the additional validation in the `sendNativeToken` and `sendWnt` functions.

Resolution

BRTR-2 | Missing Documentation

Category	Severity	Location	Status
Documentation	Low	BaseRouter.sol: 49	Pending

Description

The `sendNativeToken` function is missing NatSpec, while `sendWnt` and `sendTokens` both have the appropriate documentation.

Recommendation

Add documentation for the `sendNativeToken` function.

Resolution

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