GUARDIAN AUDITS

SMART CONTRACT SECURITY AUDIT OF

GMX

Summary

Audit Firm Guardian

Prepared By Owen Thurm, Daniel Gelfand

Client Firm GMX

Final Report Date July 28th, 2023

Audit Summary

GMX engaged Guardian to review the remediation of issues surfaced during a prior engagement in July. From the 19th of July to the 28th of July, a team of 2 auditors reviewed the source code updates. 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)	64b4b216cdae7d3d810bd58f5ae061898aedce0d

Audit Summary

Delivery Date	July 28th, 2023
Audit Methodology	Static Analysis, Manual Review, Test Suite, 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	2	0	0	2	0	0
Low	3	0	0	3	0	0

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
ADLU	AdlUtils.sol	4bf3ea9b168bbd1bd61d8ae8583145b342b867ba
BNK	Bank.sol	661c2f7e4227e315febf5800510a25a77f16bb16
SBNK	StrictBank.sol	13276745295cbc093207e92bcb096c9a01e79c99
CBKU	CallbackUtils.sol	2bb0ad384337fbbf690f9493bd55100c8bb3b9e4
DCBK	IDepositCallbackReceiver.sol	7b53a4c8082957b0f7f6aa0cc3e20d21cb1e3605
OCBK	IOrderCallbackReceiver.sol	156914da44b29805e1a5c9d5dca8160403048222
WCBK	IWithdrawalCallbackReceiver.sol	9e114c4b16376182ca7e3708c9efd708fe4d3061
ARBS	ArbSys.sol	0d9703a3477e40ccce9b0b526c0c9f4310034496
CHAIN	Chain.sol	9c435faa3ba666b16fa2054c0b39e01aa030d0a0
DATA	DataStore.sol	93a8457b50afd9dcbd1e52c7efc372c345d68971
KEY	Keys.sol	65e494a4336ef74bc632430974300976439d0b9b
DEP	Deposit.sol	9580b364ab6c14e76db4a0058a785cf10264c241
DEPS	DepositStoreUtils.sol	f6c25343cf7e26d14236ef72c25dd596d7fc30fa
EMIT	EventEmitter.sol	3fce680d9fd7432923b859ab7f9fa15e8a96ee14
DEPH	DepositHandler.sol	8228d14c7e7f1b1849ed939cae754b4b2d143499
ORDH	OrderHandler.sol	e26659e15b627b97b12057c7d874e69acc406e77
WTDH	WithdrawalHandler.sol	b87a2da08be176ffd1523148ecefa227cadb84a3
FTU	FeatureUtils.sol	4fea0cf326251322102df2ffe74c6bb663a03246
ODV	OrderVault.sol	74f991769825ba9fc8b98f3be3a5fefc32be7539
DPV	DepositVault.sol	1d19ad5afc0baec27a608a2f53cbb5b6f48f8f26

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
WDV	WithdrawalVault.sol	5cc2b331b13f735dfebc983b9aec705692e0d2a2
GSU	GasUtils.sol	e81262df819ff2a1e421de2e84fc93d5ebfca849
LIQU	LiquidationUtils.sol	740b9b5aeaad27924a1a0c72b229b6dede0007e8
MKT	Market.sol	a66a2a9127674ffb23d74d7a252f046f98c2e182
MKTF	MarketFactory.sol	b1418f56e89d4526739010caf69b937202301529
MKTS	MarketStoreUtils.sol	5f938ae585a9541bbf4f8c3561edb442694a3f46
MKTT	MarketToken.sol	a55f9a9931d906583050b4f01b74b7adbe54cf1d
MKTU	MarketUtils.sol	10a4d7ed01b9b65d8f0bc69f7c65ef70ee289153
NCU	NonceUtils.sol	6ec2082417987d5c4e859adefb9b28efb1ed5c39
PFE	IPriceFeed.sol	431babdd9ab4ee30ae9eba84f469620a3d2951f3
OCL	Oracle.sol	4771d33d54aaef1a8fe3061529d39fef8ac53f00
OCLM	OracleModule.sol	6361bd07eea14b864fce8e88ab0592b6b0e82674
OCLS	OracleStore.sol	5b87b5af1af681ee020fb0c65ddd4f184c9bef39
OCLU	OracleUtils.sol	4f386e1fc0205d5cc7cfd1dd5213f86fe78774fa
DOU	DecreaseOrderUtils.sol	a05eedf4d4b916c82ee3f76ef6f975743b7808b4
IOU	IncreaseOrderUtils.sol	a9c462ff258d7f72fdf0c337460750298709a4a5
ORD	Order.sol	fe296c4e1cba04e370a9fe576de61512bfb45b1b
BOU	BaseOrderUtils.sol	3cede11449aa54c89646c5e73af04eeab6f4c7bc
ORDS	OrderStoreUtils.sol	40ece421c2de62b0812b17b9409008cd31d8a45f
FEU	FeeUtils.sol	419e95c99abe2bfa0fafc872eff2a451cfde9740

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
ORDU	OrderUtils.sol	726ce70fd9f6fda1ca60291fb5dc9888880d34de
SWOU	SwapOrderUtils.sol	856262e9af4e709f9c433e3096d914ace4fb8c1a
DPU	DecreasePositionUtils.sol	582a9a0623226d983680fd3237be08e0271512c6
IPU	IncreasePositionUtils.sol	0b203cb45b6ab3374a1a0d5043f15047dfdb3ff6
POS	Position.sol	73596d9de7117c3c44c176ac0d2fc9627743ff9e
POSU	PositionUtils.sol	a5c87aae2b1487e7e90d745b5ffe3bf6dd51f5cf
PRICE	Price.sol	c1f87807a20c43c1710d1e3c3e628e265cd5686e
PPU	PositionPricingUtils.sol	ef8e456e9c7272b9da8a0cada726ba2172794e10
PRU	PricingUtils.sol	a1be554641c1b75b6c321baca4c9e5c722e05a53
SPRU	SwapPricingUtils.sol	5c094c9a4c742e164f38a56ea7bb83049a1b4866
READ	Reader.sol	12343e67be606e67b69ca4c8da7f9a9d6e24745e
IREFS	IReferralStorage.sol	f61d9bb3c2ec803d3b97c1e7f4faca4f1e517bf6
REFT	ReferralTier.sol	8a34d5e24b6a317b063ebd59d85fa1fec9307ea7
REFU	ReferralUtils.sol	0f761d11b0853d86db22f1a2015f4f0e03aec89b
REFS	ReferralStorage.sol	086c0102b673a95198c213003ba1e0882dbd6a87
ROLE	Role.sol	86935a3af0c782e711076d1a2ad2222bda7185fa
ROLEM	RoleModule.sol	6ff5de5a0bea585ad4195784a9f3d2013cdb935d
ROLES	RoleStore.sol	6717a28a2dc4f77505edf1a6989a559405a86883
DEPU	DepositUtils.sol	31d78e6d324c3af1d8fb65f75bda4d5d88498be2
EDPU	ExecuteDepositUtils.sol	ad21b611c2c620fe25c5743c1d2d7f5766488430

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
ERTR	ExchangeRouter.sol	2d48d92db5676c66fe2ecf7c456a7b184bcf4f79
RTR	Router.sol	0fde38bae3c62565cda7fec0ba521a46611d6e32
SWPH	SwapHandler.sol	9e3bb4bb999a70390ff2be5f447a7d4ffd5699c5
SWPU	SwapUtils.sol	02cc683fcba9ef23a8de7933a43914734f0a91a2
TIME	Timelock.sol	80359b9e696224ec3d63ab8a557548a7015ddac8
IWNT	IWNT.sol	972554584395e769df3392828d0e43adc74801f4
TU	TokenUtils.sol	dfbaa478edbc1f862cf0649d7c7f91debb82db1b
ARR	Array.sol	a27f1de5a45f6fd95f9a58f2e2a39df22208f7ff
BIT	Bits.sol	c7fa3c25af05c172cff6faccef14182665b875ba
CLC	Calc.sol	ffc7e4f0e4908afd72468dde47b7e9f7e7e3c1c4
ENM	EnumerableValues.sol	36354b53a39c4fb584313f8d3aac8e2b091d90a2
MC	BasicMulticall.sol	c23389da01002c95d775b798ccd850fa463ff6c5
PMC	PayableMulticall.sol	4af36b2f3fba97ab03e201cebb419c8897f5edd1
PREC	Precision.sol	a224e4fddc818c740c6ea87f91989d02a04c187e
WTD	Withdrawal.sol	9400ab833a8ec81c21475f30512256dd0bd5cc66
WTSU	WithdrawalStoreUtils.sol	e1bab1c92a3338dbf85bebaf7046eb2ead479343
WTDU	WithdrawalUtils.sol	17ef60c89e7e1f2e8fc5c7c414df7b60a726a38c
CBU	CallbackUtils.sol	b57c3a07448c6e5d75207ecedd36d924a4ffc575
CON	Config.sol	c47f2abda71bf0874a59aa885bbdadf3c43aa988
ERR	Errors.sol	f022e26738e729b2767192e36d733ac9c9e3e75d

Audit Scope & Methodology

ID	File	SHA-1 Checksum(s)
ERTR	BaseOrderHandler.sol	060f8d1682aa414ce853a5d82140f74eeeb6d67a
EUTL	ExchangeUtils.sol	97af1a3cbb640fa072e259f1785255ae16f96612
ERTR	LiquidationHandler.sol	3851b032bf6178455db147754536658cdd188d60
FEEH	FeeHandler.sol	f8f4e7130f55cf29db963fa40bc2dbb10e485718
MPVI	MarketPoolValueInfo.sol	63ced41c9271ea31c4ff33f1ad734c734098381a
DPSU	DecreasePositionSwapUtils.sol	c93c23fd338ceacf33110b33eb02d13bda3c5cae
PSU	PositionStoreUtils.sol	26bc7ae6b476f9afaf7b6deaf55921427813ae0f
ACC	AccountUtils.sol	2a934679f6138775382c620fd94974f87948748d
CAST	Cast.sol	68780489ad9ee795bf3d0574e96b399d36504f58
GRG	GlobalReentrancyGuard.sol	4f4a5deed4a1f00e7a349f87f5af802b85e8ba3b
MASK	Uint256Mask.sol	d5ec9bd3b5f72c11e8d93b0a4e1275f430cfdfa4
ADLH	AdlHandler.sol	9554308173b469c0b3bb9cba3e17fda56dd9c3aa
DPCU	DecreasePositionCollateralUtils.sol	cab7225c47ddb676525b7b5ea6a44e7a75a5a3f0
ERRU	ErrorUtils.sol	6e1290f8503c73a2a0f96f82d7d975aad22eb231

Audit Scope & Methodology

Vulnerability Classifications

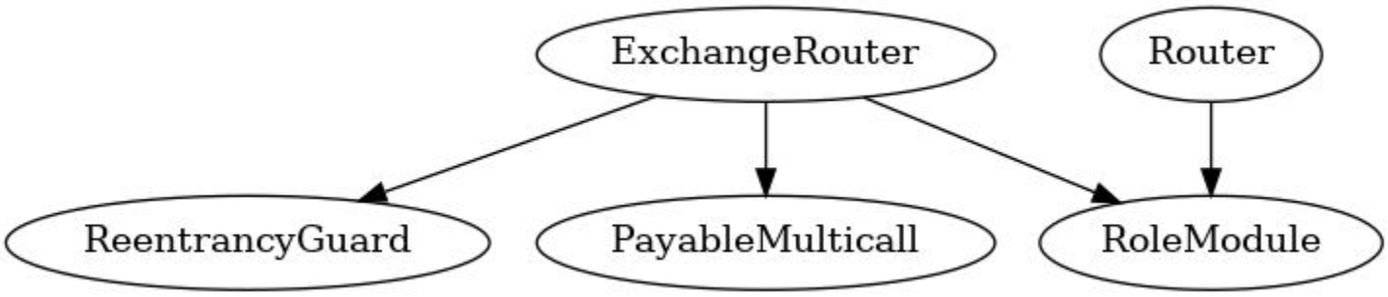
Vulnerability Level	Classification
🔴 Critical	Easily exploitable by anyone, causing loss/manipulation of assets or data.
🟠 High	Arduously exploitable by a subset of addresses, causing loss/manipulation of assets or data.
🟡 Medium	Inherent risk of future exploits that may or may not impact the smart contract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

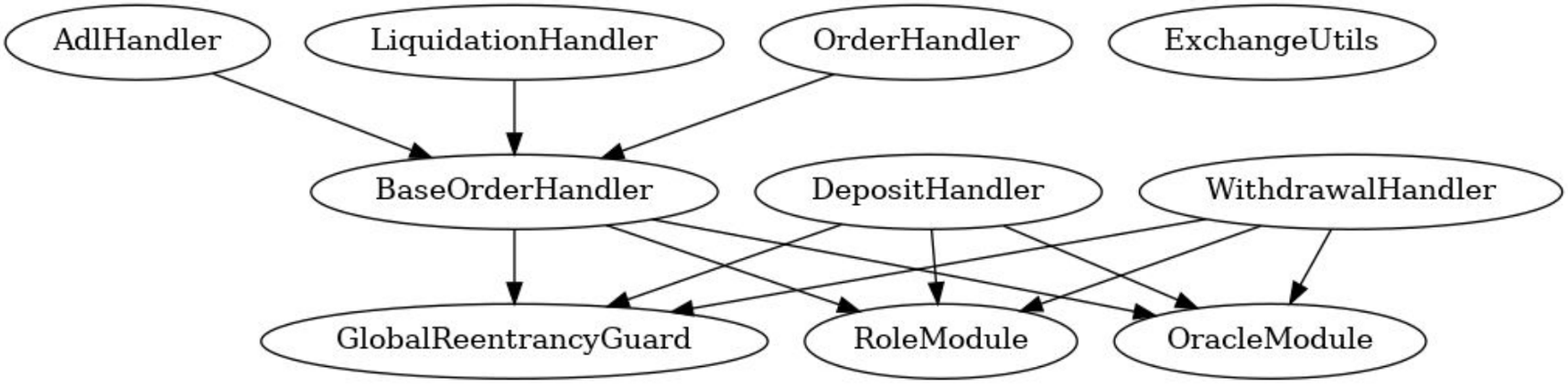
Methodology

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.

Inheritance Graph





Findings & Resolutions

ID	Title	Category	Severity	Status
GSU-1	Incorrect Decrease Gas Estimation	Logical Error	Medium	Acknowledged
GLOBAL-1	Positive Impact Misrepresented	Logical Error	Medium	Acknowledged
EDPU-1	Inefficient If Case	Optimization	Low	Acknowledged
OCL-1	Outdated NatSpec	Documentation	Low	Acknowledged
DPCU-1	Typo	Typo	Low	Acknowledged

GSU-1 | Incorrect Decrease Gas Estimation

Category	Severity	Location	Status
Logical Error	Medium	GasUtils.sol: 200-202	Acknowledged

Description

When estimating the gas needed for a decrease order in `estimateExecuteDecreaseOrderGasLimit`, 1 is added to `gasPerSwap` instead of adding 1 to the swap length to account for the extra swap due to `decreasePositionSwapType`.

Recommendation

Add 1 to the order's swap length rather than the `gasPerSwap`.

Resolution

GMX Team: The recommendation will be implemented in a future release.

GLOBAL-1 | Positive Impact Misrepresented

Category	Severity	Location	Status
Logical Error	Medium	Global	Acknowledged

Description

During both increase and decrease orders, `forPositiveImpact` is determined based upon the `priceImpactUsd` being greater than 0, however this is based on the `priceImpactUsd` after it has been capped. In the event that the position impact pool is empty and the positive price impact value is capped to 0, the fees will be calculated with a `forPositiveImpact` of `false`, meanwhile the action does indeed balance the pool.

Recommendation

Compute `forPositiveImpact` before the price impact is capped so that actions that balance the pool receive the corresponding configured fees.

Resolution

GMX Team: The recommendation will be implemented in a future release.

EDPU-1 | Inefficient If Case

Category	Severity	Location	Status
Optimization	Low	ExecuteDepositUtils.sol: 401	Acknowledged

Description

The price impact logic is split into two `if` cases where the first one accounts for positive price impact and the second accounts for negative price impact. If the first `_params.priceImpactUsd > 0` condition is met, the second `_params.priceImpactUsd < 0` condition cannot be met, however this condition is still subsequently checked.

Recommendation

Use an `else if (_params.priceImpactUsd < 0)` condition to avoid checking if the `priceImpactUsd` is negative if it was already found to be positive.

Resolution

GMX Team: Acknowledged.

OCL-1 | Outdated NatSpec

Category	Severity	Location	Status
Documentation	Low	Oracle.sol: 56-65	Acknowledged

Description

The NatSpec does not match the struct parameters. Missing parameters include:

- info
- minBlockConfirmations
- maxRefPriceDeviationFactor
- validatedPrices

Recommendation

Update the NatSpec to reflect the struct accurately.

Resolution

GMX Team: NatSpec will be updated in a future release.

DPCU-1 | Typo

Category	Severity	Location	Status
Typo	Low	DecreasePositionCollateralUtils.sol: 590-593	Acknowledged

Description

"[t]he difference would be in the stored as a…" should be edited to "the difference would be stored as".

Recommendation

Edit the comment described above.

Resolution

GMX Team: The typo will be fixed in a future release.

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