



SOLIDProof

Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

DMX DAO

Audit

Security Assessment
07. April, 2023

For



SolidProof_io



@solidproof_io

Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Links	5
Methodology	8
Used Code from other Frameworks/Smart Contracts (direct imports)	9
Tested Contract Files	10
Source Lines	19
Risk Level	19
Capabilities	20
Inheritance Graph	21
CallGraph	22
Scope of Work/Verify Claims	23
Modifiers and public functions	25
Source Units in Scope	26
Critical issues	30
High issues	30
Medium issues	30
Low issues	30
Informational issues	30
Audit Comments	31
SWC Attacks	32

Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	31. March 2023 - 6. April 2023	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Fantom Blockchain

Website

<https://dmxdao.com/>

Telegram

https://t.me/DMX_Community

Twitter

<https://twitter.com/DmxDao>

Medium

<https://medium.com/@DMXDAO>



Description

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

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

Project Engagement

During the 31th of March 2023, **DMX DAO Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Links

v1.0

DMX: [0x0Ec581b1f76EE71FB9FEefd058E0eCf90EBAAb63E](https://etherscan.io/address/0x0Ec581b1f76EE71FB9FEefd058E0eCf90EBAAb63E)

Vault: [0xD093eeE7c968CEef2df96cA9949eba1a1A9b2306](https://etherscan.io/address/0xD093eeE7c968CEef2df96cA9949eba1a1A9b2306)

Router: [0xE9a5FfCE7596AACf0Cb7fAF1e084fD2B59838C0B](https://etherscan.io/address/0xE9a5FfCE7596AACf0Cb7fAF1e084fD2B59838C0B)

PositionRouter: [0x42bb8B3b8d60A3e58B9F10D67AfCff5DE54F26eD](https://etherscan.io/address/0x42bb8B3b8d60A3e58B9F10D67AfCff5DE54F26eD)

OrderBook: [0xeD077045f38f864fba8aD9bdbF1CE8F108e5ddb9](https://etherscan.io/address/0xeD077045f38f864fba8aD9bdbF1CE8F108e5ddb9)

Reader: [0xC5EAC26893224E0BCB9a685aa0b82446a48a944E](https://etherscan.io/address/0xC5EAC26893224E0BCB9a685aa0b82446a48a944E)

OrderBookReader: [0x75A29e4D607a426440ae88B44AF18B562D246022](https://etherscan.io/address/0x75A29e4D607a426440ae88B44AF18B562D246022)

DlpManager: [0xd2b6784b8302D0705a90B720d18E16362EFbda76](https://etherscan.io/address/0xd2b6784b8302D0705a90B720d18E16362EFbda76)

RewardRouter: [0x3136A318F40Cffc7b75cea83A4F6FB0C372E4922](https://etherscan.io/address/0x3136A318F40Cffc7b75cea83A4F6FB0C372E4922)

GitHub- <https://github.com/dmxdao/damx-protocol>
Commit: c5efdf1



Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

The contract is an identical fork of GMX and have the same imports and libraries



Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

File Name	SHA-1 Hash
contracts/staking/ StakedGlpMigrator.sol	40a75eb4fe0e4216edb632263 7f438352c8587ff
contracts/staking/GlpBalance.sol	f812ec71143d27a31847b04fb 0bf8f3e390dafce
contracts/staking/ RewardRouterV2.sol	541de87a0b89c0c0574920f66 97a5a168f4c1f25
contracts/libraries/math/Math.sol	c39054602f9a9c506e0d7806c da05fb53155cae5
contracts/libraries/math/ UQ112x112.sol	f97edb26adf392a66e467e646 0b2e6b2aa34a3d7
contracts/libraries/math/SafeMath.sol	77b960c856f29c76aa78767f9 66de67f8b739454
contracts/oracle/PriceFeed.sol	137c096402a1ef4737cda876d 92530833fe47d61
contracts/oracle/FastPriceEvents.sol	51b56e6a847cce4a147056a5 ac8800c4fef6ef24
contracts/oracle/FastPriceFeed.sol	83f5c3e5d435fd1aa2a968451 ae33aebc1ea3885
contracts/tokens/YieldFarm.sol	1b4bceec6cc9e055e5330b2c9 d28096c0db7368e
contracts/tokens/YieldTracker.sol	98cc93c94e66e7b4174e9a14 3b227ba5ae54c6a2

contracts/tokens/YieldToken.sol	d61334487af72819ad4d7211b7b0f00512ea7d88
contracts/tokens/TimeDistributor.sol	0eaecfde7cb997c61a02ffb1ae26e0e53fed7f45
contracts/tokens/Token.sol	7b671c4619396166b449f2d87bb281a803ecc245
contracts/staking/BonusDistributor.sol	ed72905fd8b9c2bb3d8f1b34e78bd35b14a09c39
contracts/tokens/USDG.sol	644862d4a48b9aa11a2a65acf93758bfff8f11c9
contracts/peripherals/ PriceFeedTimelock.sol	d091742cb818df7e4667ebdf802270ebcecbad5a
contracts/staking/interfaces/ IRewardDistributor.sol	6165aef87d3a390a96107dbc015b2d5bd2aaa941
contracts/peripherals/ EsGmxBatchSender.sol	0bc2bca8553d65a073c6089b1e3ef767be978bc6
contracts/oracle/interfaces/ IChainlinkFlags.sol	6d99a297b10e29f4000a7fc2f8c131d2ce069be2
contracts/peripherals/ GmxTimelock.sol	1c7623593a567e9f9b62b18d38d7ddec04ce3e0c
contracts/libraries/introspection/ IERC165.sol	21852df340c01e66c1efda22d8fa48417f08c814
contracts/staking/interfaces/ IRewardRouterV2.sol	f43c18b2d9d43e68d5b0c24a3d31eb62e799ce61
contracts/peripherals/ OrderBookReader.sol	b3ee4edf3351f8244a6df5d9976fc73ee77f9b3e
contracts/gambit-token/interfaces/ IGMT.sol	3b20d9d683f236f9b0453a11b4a6e06994ef1fc4
contracts/tokens/BaseToken.sol	2ab07293ea5f7fd49f2ad31026fcb097db56c283

contracts/libraries/introspection/ ERC165.sol	29a66d5bc5dbfbbebd739267db d61c24b84919e25
contracts/peripherals/ RewardReader.sol	e11989dee441e95fe2fcd0235 e9c33e253191fac
contracts/staking/interfaces/ IRewardTracker.sol	c9ea55c4c6c74cc6fc8c5ab00 e37fe4481515bcb
contracts/referrals/ReferralReader.sol	5b9cf7c82fbd8155a6cd42e76c 76328104f741d0
contracts/tokens/ MintableBaseToken.sol	12e55334d799c6a9b24e7f99b 7208bd409097b97
contracts/peripherals/ BalanceUpdater.sol	37278011aad8478ad5046a9a a604f5261fd99721
contracts/tokens/WETH.sol	2da9af6a09db8acb1fad8f82f0 7e82339ae6b46d
contracts/peripherals/Timelock.sol	e7ad9cd7b17a16d28c2513e0 bd03d3cf600ca593
contracts/referrals/ReferralStorage.sol	87d0be4b6a5b35cc97ecfb7c9 0876f74a5575646
contracts/tokens/Bridge.sol	35f60d14b4a7cec6a1b28330e ee6232b9f14fcdf
contracts/peripherals/Reader.sol	a39078fe9dc5f95ff907292ba5 d096878b48f3fe
contracts/oracle/interfaces/ IFastPriceFeed.sol	5a0b9c59198b76ccda704846 9d771c7482f1435f
contracts/staking/interfaces/ IVester.sol	9cc838d160a5c5e71943544a 666cee56c4c85619
contracts/peripherals/ ShortsTrackerTimelock.sol	4c8b074d29ffde48fc807ade97 02395804d5bd76
contracts/peripherals/VaultReader.sol	3d3ffd9ad412b0c7a353136bcf e8fe44d7208246

contracts/peripherals/BatchSender.sol	6846a9ec48924767b4386d616b8f4551a798fb5a
contracts/gambit-token/Treasury.sol	35c283f8b5f7aefdc0145522b007fdc025e973f3
contracts/gambit-token/GMT.sol	b9ac165178dfb9c12f0624e267a31b28af8cb423
contracts/staking/StakedGlp.sol	f45974718453fa1909dafa03fb72cd4bf5625f44
contracts/oracle/interfaces/ IFastPriceEvents.sol	99ac2e248cdc92441bab30a952b191726beb3bda
contracts/oracle/interfaces/ ISecondaryPriceFeed.sol	a6b76377a445e30447d5a0d48eba5ec85fd333fa
contracts/oracle/interfaces/ IPriceFeed.sol	b6695b7784849790b2f7544c74365741c0e2c9c7
contracts/referrals/interfaces/ IReferralStorage.sol	9c47db454e13c8f69cfe0dc6009230f661677498
contracts/staking/StakeManager.sol	1b5a78374c09f6a12b186cca36e3d2733fe5b853
contracts/staking/Vester.sol	b2250a623c07a86a0d2a06ee9b0f0bdf6b85fa51
contracts/staking/ RewardDistributor.sol	0662464a90b793e3ed16928f81e99e476e6fc6de
contracts/libraries/access/ Ownable.sol	3b8b43b96279a54053561e606ce9ff220b7c6a0a
contracts/amm/PancakePair.sol	d251aa72ef71b34a23ebed93978c6eac2fa6ff9e
contracts/amm/UniFactory.sol	7868887c450d9a7bf00bb2fcd4f8f461d5093f87
contracts/amm/PancakeRouter.sol	b133fbd7d310dfd1978b9bbd6e3dab7a510347d8

contracts/amm/UniPool.sol	bbc6dc2247b3f19f38b9a2dfa2ea891487e756a2
contracts/amm/UniNftManager.sol	cc48523f89cddce0ad84bd8311bc7d9a57f117a5
contracts/staking/RewardTracker.sol	b40b1cd6cd1c35a23f1abc4505765c0b5a03e078
contracts/staking/RewardRouter.sol	fa9e85c1dbe8863c5fbe652173b8735208a10bb7
contracts/amm/PancakeFactory.sol	b85332f48ecf949add7d5ad8717115919c82a6d3
contracts/peripherals/interfaces/ ITimelock.sol	212174462e86b1c0b74aa61ef60a02200acc2abc
contracts/peripherals/interfaces/ ITimelockTarget.sol	0c1c4578897fc45f0ba57cc8d2d8a4ffbe63afeb
contracts/peripherals/interfaces/ IGmxTimelock.sol	e86bb0eb492d5d8db803cebbe0dd5366671fb2a8
contracts/peripherals/interfaces/ IHandlerTarget.sol	0a2a4fd80b2fda94ea9685c02ca0df999179fe20
contracts/libraries/GSN/Context.sol	ae89f5593a48ee0e86398ad6ef981f515674ec12
contracts/tokens/SnapshotToken.sol	44777d96c971738976785a755bea38d58e32f9c7
contracts/libraries/utils/ EnumerableMap.sol	c2fa7432211f3b4381688359ed316dcd30767d41
contracts/amm/interfaces/ IPancakeRouter.sol	af1d67a298fab838536be9d0d4a507b484e7bf21
contracts/amm/interfaces/ IPancakePair.sol	a2b07ac4925605264c2cb0cb83c14827c34533fd
contracts/amm/interfaces/ IPancakeFactory.sol	8133c5b9cd563ab335695f58e1e05c31bd08910f

contracts/libraries/utis/Strings.sol	444a4b378eeb1b3a7ac60150 0210f2b09bb1d7b2
contracts/access/Governable.sol	ba5f82a34c23ede5e592cabe2 dfb5c9285f90e08
contracts/libraries/utis/ EnumerableSet.sol	ff28b75e68496eff70710d1dad 8e7699a7371540
contracts/tokens/FaucetToken.sol	d50c187cc161c8be0ba4fe2fdd 342de1219f4ebd
contracts/access/TokenManager.sol	fa5a9401cfb3eb559df185b324 f4d843d42c9435
contracts/libraries/utis/Address.sol	40ba11bb4b1e3ff517e21bb12 3913b65690215c5
contracts/libraries/utis/ ReentrancyGuard.sol	49394da5ad4c91f2b42f00b73 84dbf3f2cfa4b94
contracts/gmx/GmxFloor.sol	1a68a4a76a1d111050a03221 581efcd5a3b17de2
contracts/gmx/GLP.sol	df341545447df4bdcd481624e bc0d8ea7de0f9f1
contracts/gmx/GMX.sol	aad72ec39ec2568dc2c7d3320 9a05be4d9081e44
contracts/gmx/MigrationHandler.sol	8448b4fd227228c5b505b01d2 36c0eb233283684
contracts/access/interfaces/ IAdmin.sol	ed2e089186d08606f9a422db1 2e274277ad4dded
contracts/gmx/EsGMX.sol	1d37c610465abc8f07e6bd729 8345e15f12ab2ab
contracts/gmx/GmxMigrator.sol	02bbee26ba7733017ab6e406 7672ab12d6729ed3
contracts/gmx/Gmxlou.sol	1ceb0b1f85e208b745086f101 318090fc76354fe

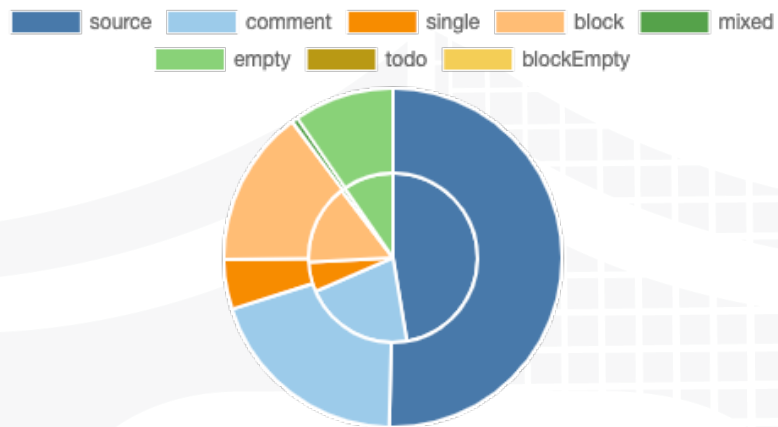
contracts/libraries/token/ SafeERC20.sol	494c092678a64d33825396ebf 9ff0625f5fb307d
contracts/libraries/token/ERC20.sol	223536578c8b208b540ce362 c36f8a7ea5d2478b
contracts/libraries/token/IERC20.sol	dcf4f07f947c93d5949a5fd780 3e411db32a7c21
contracts/tokens/interfaces/ IYieldToken.sol	bd0ab606e47640983d81ee5f6 e978458bad5e6df
contracts/tokens/interfaces/ IDistributor.sol	20b7401e157fb33da458b50ee d205ecac6a174ac
contracts/tokens/interfaces/ IMintable.sol	360dbd26eb04be76c89ce6a4f 24e4f07b890d7db
contracts/tokens/interfaces/IUSDG.sol	269d4e7e802a2d9dc56c9d8a 175664a5c369cc2c
contracts/tokens/interfaces/ IWETH.sol	0993cb783747efce3a82ce671 449901ad71be1e5
contracts/libraries/token/ERC721/ IERC721.sol	37a39b62a3f38c5ad1545a6dd 08c976e53dff646
contracts/tokens/interfaces/ IYieldTracker.sol	0a56ce7f21299450fbbbf07830 7fdf76ba542251
contracts/tokens/interfaces/ IBaseToken.sol	8907934faad88399fa11d5b5c cb5b85e0abc61bc
contracts/libraries/token/ERC721/ ERC721.sol	0ed1800f6b2884b12e5a652ae fc9e41d49d9390a
contracts/tokens/interfaces/IBridge.sol	12e96b9eaaa8e39bcb2b595cf bedd44487fb0c7d
contracts/tokens/interfaces/IGLP.sol	cb4c850cf1a80ad9916724af8 77cd60a4bf9c339
contracts/libraries/token/ERC721/ IERC721Receiver.sol	085af91f67db310c21f684722d 8d5a8e488fefeb

contracts/libraries/token/ERC721/ IERC721Metadata.sol	9ca42611901c231b4acd37d67 184048456113955
contracts/libraries/token/ERC721/ IERC721Enumerable.sol	63b8e526b2a490c58af723147 04125d19023f8cc
contracts/gmx/interfaces/ IAmmRouter.sol	8c1039087c4d7a469185cab5 7e57ce3e79ded4f0
contracts/core/Vault.sol	3e28d7e70617ecc434e075aa 390f7d33a1a77db7
contracts/core/PositionUtils.sol	36fb734ac51ba2f4dc9959ecf3 db8c98da830744
contracts/gmx/interfaces/ IGmxMigrator.sol	da7d65044045e958cac4b4dc 2d6982b9d76aab03
contracts/gmx/interfaces/IGmxlou.sol	b1bf8e3091a6e4252ba680dd1 1e341d11aa6f005
contracts/core/VaultUtils.sol	aef40009826863374c7774747 428fd0b44bc9da1
contracts/core/interfaces/ IPositionRouter.sol	d90d14592b63224485b4a143 40ea2f6e5c357c5a
contracts/core/interfaces/ IPositionRouterCallbackReceiver.sol	7a52db1d3393b13a5df4c0fe3 76c12a3fe1d6a6e
contracts/core/interfaces/ IShortsTracker.sol	ab9081b0bb4ce63cb0202cbb 0c2dd71fb29367f0
contracts/core/interfaces/IRouter.sol	77d61cbe59c4f2c3ab13b9f95 e31ec7163ff3e67
contracts/core/interfaces/ IVaultPriceFeed.sol	57d0d7557e67e7d5255a28bd e2184a57d919c97a
contracts/core/interfaces/ IOrderBook.sol	cc9690514916d87a46bbb2b4 1e064a6a19e13f64
contracts/core/interfaces/ IGlpManager.sol	10be398b1b704364462808e1 5d3ee32747be81f7

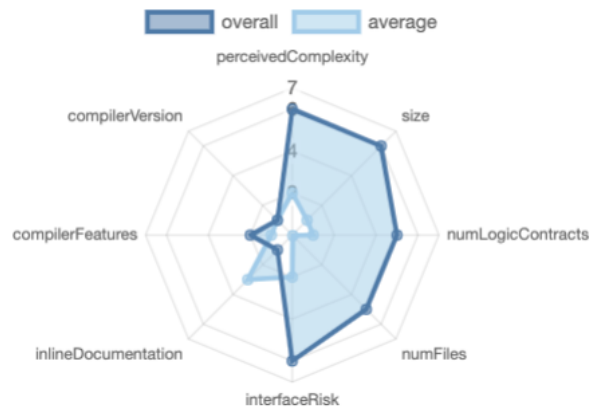
contracts/core/interfaces/ IVaultUtils.sol	03ce6c770c92493496409bab b9982cd989637800
contracts/core/interfaces/IVault.sol	30982a3eeee189177a5acc88 b3eff16bbc98437e
contracts/core/interfaces/ IBasePositionManager.sol	3325a49c5ed13dee4456e561 b4cbf2afd9ab5fcf
contracts/core/PositionManager.sol	eb06d5a59d89e0e8685a456a d464526541576a60
contracts/core/OrderBook.sol	671f307a6bca346ee32e63b97 0f161e5cc2c6159
contracts/core/ShortsTracker.sol	6f5d8f11c71c45c10e51a476a8 9c6c04bc680626
contracts/core/PositionRouter.sol	8b19fa1192bdcc1bea583053c 96848d296c60979
contracts/core/VaultPriceFeed.sol	50749ba34d69357e4d240dedf c1d5cb31502964c
contracts/core/GlpManager.sol	beb704b46c6ffef75f9d11b9ab 477691cc34adf6
contracts/core/Router.sol	fcc301a043e3e97162c354909 72b40ab73938e76
contracts/core/VaultErrorController.sol	007dd87b11df74513362f534a 510037839d6d955
contracts/core/ BasePositionManager.sol	3ea6b190b4ff2ad146852c71b 560cb1bdc287cca

Metrics

Source Lines v1.0



Risk Level v1.0



Capabilities

Components

 Contracts	 Libraries	 Interfaces	 Abstract
71	9	47	1


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.





 Public	 Payable
1128	19







External	Internal	Private	Pure	View
846	1065	130	24	390

StateVariables

Total	 Public
574	524

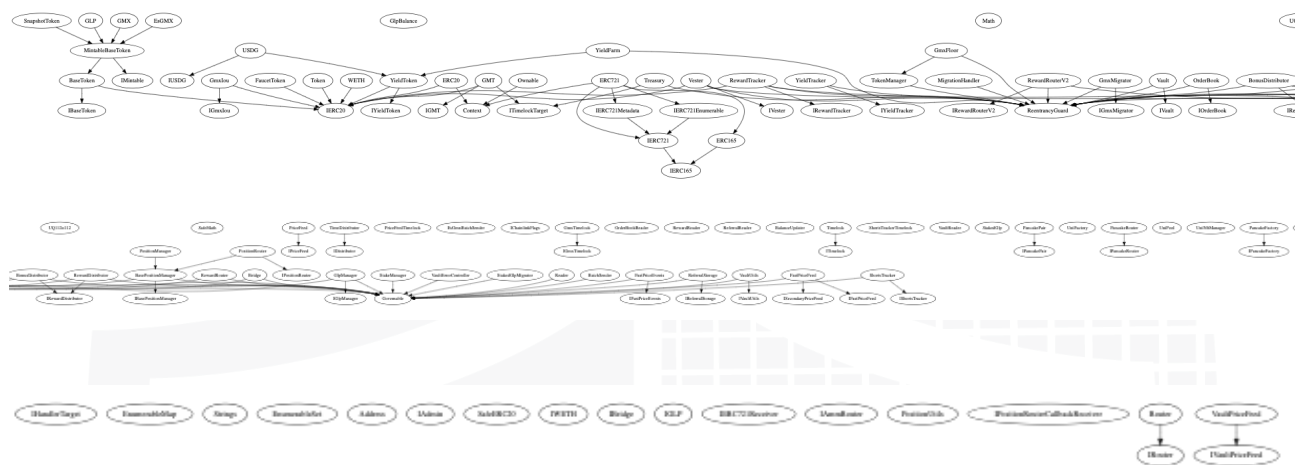
Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
0.6.12 ^0.6.0 >=0.5.0 ^0.6.2	ABIEncoderV2	yes	yes (2 asm blocks)	

 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECREcover	 New/Create/Create2
yes		yes	yes		

 TryCatch	Σ Unchecked
yes	

Inheritance Graph v1.0





Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Overall checkup (Smart Contract Security)



Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚠
Unverified / Not checked	✗
Not available	—

Modifiers and public functions

v1.0

Note:

- Identical fork from GMX
- GMX
 - Contracts inside are the same as the gmx-contracts directory
 - <https://github.com/gmx-io/gmx-contracts/tree/master/contracts>

Ownership Privileges

- N/A

Please check if an OnlyOwner or similar restrictive modifier has been forgotten.

Source Units in Scope

v1.0

File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score
contracts/staking/StakedGlpMigrator.sol	1	—————	59	59	41	5	30
contracts/staking/GlpBalance.sol	1	—————	68	68	50	1	34
contracts/staking/RewardRouterV2.sol	1	—————	423	401	296	3	365
contracts/libraries/math/Math.sol	1	—————	25	25	18	3	5
contracts/libraries/math/UQ112x112.sol	1	—————	22	22	10	7	4
contracts/libraries/math/SafeMath.sol	1	—————	159	159	39	106	10
contracts/oracle/PriceFeed.sol	1	—————	51	49	35	2	25
contracts/oracle/FastPriceEvents.sol	1	—————	23	23	15	1	13
contracts/oracle/FastPriceFeed.sol	1	—————	476	468	330	35	292
contracts/tokens/YieldFarm.sol	1	—————	29	29	20	1	22
contracts/tokens/YieldTracker.sol	1	—————	117	117	85	7	80
contracts/tokens/YieldToken.sol	1	—————	220	220	166	2	146
contracts/tokens/TimeDistributor.sol	1	—————	124	120	89	1	68
contracts/tokens/Token.sol	1	—————	327	327	105	185	97
contracts/staking/BonusDistributor.sol	1	—————	94	94	68	2	64
contracts/tokens/USDG.sol	1	—————	36	36	25	1	24
contracts/peripherals/PriceFeedTimelock.sol	1	—————	302	290	234	1	219
contracts/staking/interfaces/IRewardDistributor.sol	—————	1	10	6	3	1	9
contracts/peripherals/EsGmxBatchSender.sol	1	—————	60	55	38	1	34
contracts/oracle/interfaces/IChainlinkFlags.sol	—————	1	7	6	3	1	3
contracts/peripherals/GmxTimelock.sol	1	—————	563	514	422	5	378
contracts/libraries/introspection/IERC165.sol	—————	1	24	23	3	18	3
contracts/staking/interfaces/IRewardRouterV2.sol	—————	1	8	6	3	1	5
contracts/peripherals/OrderBookReader.sol	1	—————	143	131	98	4	106
contracts/gambit-token/interfaces/IGMT.sol	—————	1	8	6	3	1	5
contracts/tokens/BaseToken.sol	1	—————	223	223	169	2	148
contracts/libraries/introspection/ERC165.sol	1	—————	54	54	16	31	9
contracts/peripherals/RewardReader.sol	1	—————	58	58	50	1	80
contracts/staking/interfaces/IRewardTracker.sol	—————	1	19	6	3	1	27
contracts/referrals/ReferralReader.sol	1	—————	18	18	12	1	20
contracts/tokens/MintableBaseToken.sol	1	—————	31	31	21	1	21
contracts/peripherals/BalanceUpdater.sol	1	—————	30	25	18	1	14
contracts/tokens/WETH.sol	1	—————	322	322	103	185	90
contracts/peripherals/Timelock.sol	1	—————	618	574	463	7	457
contracts/referrals/ReferralStorage.sol	1	—————	119	119	89	5	62
contracts/tokens/Bridge.sol	1	—————	38	38	27	2	30
contracts/peripherals/Reader.sol	1	—————	398	398	329	4	454
contracts/oracle/interfaces/IFastPriceFeed.sol	—————	1	20	6	3	1	29
contracts/staking/interfaces/IVester.sol	—————	1	28	6	3	1	37
contracts/peripherals/ShortsTrackerTimelock.sol	1	—————	230	230	168	1	162
contracts/peripherals/VaultReader.sol	1	—————	76	76	63	1	78
contracts/peripherals/BatchSender.sol	1	—————	52	52	38	1	26
contracts/gambit-token/Treasury.sol	1	—————	169	166	126	11	131

contracts/gambit-token/GMT.sol	1	—————	163	163	111	13	97
contracts/staking/StakedGlp.sol	1	—————	97	97	70	4	53
contracts/oracle/interfaces/IFastPriceEvents.sol	—————	1	7	6	3	1	3
contracts/oracle/interfaces/ISecondaryPriceFeed.sol	—————	1	7	6	3	1	3
contracts/oracle/interfaces/IPriceFeed.sol	—————	1	11	6	3	1	11
contracts/referrals/interfaces/IReferralStorage.sol	—————	1	15	6	3	1	19
contracts/staking/StakeManager.sol	1	—————	17	12	8	1	8
contracts/staking/Vester.sol	1	—————	377	377	277	11	229
contracts/staking/RewardDistributor.sol	1	—————	83	83	61	2	50
contracts/libraries/access/Ownable.sol	1	—————	68	68	27	33	23
contracts/amm/PancakePair.sol	1	—————	23	23	17	4	13
contracts/amm/UniFactory.sol	1	—————	7	7	4	1	2
contracts/amm/PancakeRouter.sol	1	—————	37	28	19	3	15
contracts/amm/UniPool.sol	1	—————	35	31	17	10	6
contracts/amm/UniNftManager.sol	1	—————	51	34	28	2	10
contracts/staking/RewardTracker.sol	1	—————	306	303	223	4	212
contracts/staking/RewardRouter.sol	1	—————	272	260	187	3	210
contracts/amm/PancakeFactory.sol	1	—————	33	33	25	1	15
contracts/peripherals/interfaces/ITimelock.sol	—————	1	12	6	3	1	13
contracts/peripherals/interfaces/ITimelockTarget.sol	—————	1	8	6	3	1	5
contracts/peripherals/interfaces/IGmxTimelock.sol	—————	1	9	6	3	1	7
contracts/peripherals/interfaces/IHandlerTarget.sol	—————	1	8	6	3	1	5
contracts/libraries/GSN/Context.sol	1	—————	24	24	10	12	1
contracts/tokens/SnapshotToken.sol	1	—————	18	18	13	1	15
contracts/libraries/utills/EnumerableMap.sol	1	—————	237	237	81	130	30
contracts/amm/interfaces/IPancakeRouter.sol	—————	1	16	6	3	1	3
contracts/amm/interfaces/IPancakePair.sol	—————	1	7	6	3	1	3
contracts/amm/interfaces/IPancakeFactory.sol	—————	1	7	6	3	1	3
contracts/libraries/utills/Strings.sol	1	—————	34	34	22	9	18
contracts/access/Governable.sol	1	—————	20	20	14	1	8
contracts/libraries/utills/EnumerableSet.sol	1	—————	243	243	77	136	29
contracts/tokens/FaucetToken.sol	1	—————	350	350	125	185	103
contracts/access/TokenManager.sol	1	—————	230	230	188	1	196
contracts/libraries/utills/Address.sol	1	—————	189	169	78	113	47
contracts/libraries/utills/ReentrancyGuard.sol	1	—————	62	62	15	38	5
contracts/gmx/GmxFloor.sol	1	—————	116	116	85	3	82
contracts/gmx/GLP.sol	1	—————	14	14	9	1	8
contracts/gmx/GMX.sol	1	—————	14	14	9	1	8
contracts/gmx/MigrationHandler.sol	1	—————	159	136	107	2	107
contracts/access/interfaces/IAdmin.sol	—————	1	7	6	3	1	3
contracts/gmx/EsGMX.sol	1	—————	14	14	9	1	8
contracts/gmx/GmxMigrator.sol	1	—————	239	225	175	1	161
contracts/gmx/Gmxlou.sol	1	—————	66	66	45	9	36
contracts/libraries/token/SafeERC20.sol	1	—————	75	74	33	32	25
contracts/libraries/token/ERC20.sol	1	—————	306	306	89	185	81
contracts/libraries/token/IERC20.sol	—————	1	77	26	17	57	13
contracts/tokens/interfaces/IYieldToken.sol	—————	1	9	6	3	1	7
contracts/tokens/interfaces/IDistributor.sol	—————	1	10	6	3	1	9
contracts/tokens/interfaces/IMintable.sol	—————	1	10	6	3	1	9
contracts/tokens/interfaces/IUSDG.sol	—————	1	10	6	3	1	9
contracts/tokens/interfaces/IWETH.sol	—————	1	9	6	3	1	10

contracts/libraries/token/ERC721/ERC721.sol	—————	1	129	62	40	99	21
contracts/tokens/interfaces/IYieldTracker.sol	—————	1	10	6	3	1	9
contracts/tokens/interfaces/IBaseToken.sol	—————	1	11	6	3	1	11
contracts/libraries/token/ERC721/ERC721.sol	1	—————	477	464	173	222	161
contracts/tokens/interfaces/IBridge.sol	—————	1	8	6	3	1	5
contracts/tokens/interfaces/IGLP.sol	—————	1	8	6	3	1	5
contracts/libraries/token/ERC721/ERC721Receiver.sol	—————	1	21	20	3	15	3
contracts/libraries/token/ERC721/ERC721Metadata.sol	—————	1	27	16	4	14	9
contracts/libraries/token/ERC721/ERC721Enumerable.sol	—————	1	29	20	8	16	9
contracts/gmx/interfaces/IAMMRouter.sol	—————	1	23	6	3	1	5
contracts/core/Vault.sol	1	—————	1236	1211	898	96	662
contracts/core/PositionUtils.sol	1	—————	84	65	39	7	37
contracts/gmx/interfaces/IGmxMigrator.sol	—————	1	7	6	3	1	3
contracts/gmx/interfaces/IGmxLou.sol	—————	1	7	6	3	1	3
contracts/core/VaultUtils.sol	1	—————	171	171	122	22	113
contracts/core/interfaces/IPositionRouter.sol	—————	1	10	6	3	1	9
contracts/core/interfaces/IPositionRouterCallbackReceiver.sol	—————	1	7	6	3	1	3
contracts/core/interfaces/IShortsTracker.sol	—————	1	27	6	3	1	13
contracts/core/interfaces/IRouter.sol	—————	1	11	6	3	1	11
contracts/core/interfaces/IVaultPriceFeed.sol	—————	1	27	6	3	1	33
contracts/core/interfaces/IOrderBook.sol	—————	1	44	6	3	1	13
contracts/core/interfaces/IGlpManager.sol	—————	1	20	8	4	1	25
contracts/core/interfaces/IVaultUtils.sol	—————	1	17	6	3	1	23
contracts/core/interfaces/IVault.sol	—————	1	128	8	4	1	169
contracts/core/interfaces/IBasePositionManager.sol	—————	1	8	6	3	1	5
contracts/core/PositionManager.sol	1	—————	314	259	190	20	195
contracts/core/OrderBook.sol	1	—————	984	871	745	27	310
contracts/core/ShortsTracker.sol	1	—————	221	189	138	11	108
contracts/core/PositionRouter.sol	1	—————	790	727	583	18	241
contracts/core/VaultPriceFeed.sol	1	—————	380	375	279	21	237
contracts/core/GlpManager.sol	1	—————	260	260	200	5	202
contracts/core/Router.sol	1	—————	221	221	176	5	177
contracts/core/VaultErrorController.sol	1	—————	15	15	11	1	12
contracts/core/BasePositionManager.sol	1	—————	327	316	243	8	153
Totals	81	47	16158	15023	10131	2303	8957

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalised lines of the source unit (e.g. normalises functions spanning multiple lines)
nSLOC	normalised source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments

Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)
------------------	---



Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

Issue	File	Type	Line	Description
#1	All	Multiple pragma is set	—	Some of the contracts contain different pragma versions which is not recommended for deployment. We recommend to have the same pragma in all contracts and also to update the old pragma versions to the new ones.
#2	All	Old Compiler Version	—	The contracts use a very old compiler version which is not recommended for deployment as it is susceptible to known vulnerabilities

Informational issues

Issue	File	Type	Line	Description
#1	All	Contract doesn't import npm packages from source (like OpenZeppelin etc.)	—	We recommend importing all packages from npm directly without flattening the contract. Functions could be modified or can be susceptible to vulnerabilities

Audit Comments

We recommend you to use the special form of comments (NatSpec Format, Follow link for more information <https://docs.soliditylang.org/en/latest/natspec-format.html>) for your contracts to provide rich documentation for functions, return variables and more. This helps investors to make clear what that variables, functions etc. do.

07. April 2023:

- This project consists of the following forks
 - GMX
- Read whole report and modifiers section for more information
- The low issues that exist in the GMX codebase still exist in the forked code.
- We recommend using a multisig wallet for the owner address to prevent any risk of the loss of private key
- Do your own research here

SWC Attacks

ID	Title	Relationships	Status
SW C-1 36	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-1 35	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-1 34	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-1 33	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-1 32	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-1 31	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SW C-1 30	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-1 29	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-1 28	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SW C-1 27	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SW C-1 25	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SW C-1 24	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SW C-1 23	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SW C-1 22	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SW C-1 21	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SW C-1 20	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SW C-11 9	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-11 8	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SW C-11 7	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SW C-11 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SW C-11 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SW C-11 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SW C-11 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SW C-11 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SW C-1 09	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-1 08	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-1 07	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-1 06	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SW C-1 05	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SW C-1 04	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SW C-1 03	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	NOT PASSED
SW C-1 02	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	NOT PASSED
SW C-1 01	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SW C-1 00	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

*Solid
Proofed*

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**


MADE IN GERMANY