RUBIC SECURITY AUDIT REPORT

March 30, 2023

MixBytes()

TABLE OF CONTENTS

1. INTRODUCTION 2

1.1 Disclaimer 2

1.2 Security Assessment Methodology 2

1.3 Project Overview 5

1.4 Project Dashboard 5

1.5 Summary of findings 22

1.6 Conclusion 23

2.FINDINGS REPORT 24

2.1 Critical 24

C-1 Incorrect blacklisting of unsafe calls 24

C-2 Arbitrary calls execution in `Executor` and `GenericCrossChainFacet` 25

2.2 High 26

2.3 Medium 26

M-1 Unsafe practice of managing a user's ERC20 approve 26

M-2 The administrator can modify trusted functionality 27

2.4 Low 28

L-1 Unused logic 28

2.5 Appendix 29

1. Monitoring recommendation 29

3. ABOUT MIXBYTES 30

1. INTRODUCTION

1.1 Disclaimer

The audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, investment advice, endorsement of the platform or its products, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only. The information presented in this report is confidential and privileged. If you are reading this report, you agree to keep it confidential, not to copy, disclose or disseminate without the agreement of the Client. If you are not the intended recipient(s) of this document, please note that any disclosure, copying or dissemination of its content is strictly forbidden.

1.2 Security Assessment Methodology

A group of auditors are involved in the work on the audit. The security engineers check the provided source code independently of each other in accordance with the methodology described below:

1. Project architecture review:

- Project documentation review.
- General code review.
- Reverse research and study of the project architecture on the source code alone.

Stage goals
- Build an independent view of the project's architecture.
- Identifying logical flaws.

2. Checking the code in accordance with the vulnerabilities checklist:

- Manual code check for vulnerabilities listed on the Contractor's internal checklist. The Contractor's checklist is constantly updated based on the analysis of hacks, research, and audit of the clients' codes.
- Code check with the use of static analyzers (i.e Slither, Mythril, etc).

Stage goal

Eliminate typical vulnerabilities (e.g. reentrancy, gas limit, flash loan attacks etc.).

3. Checking the code for compliance with the desired security model:

- Detailed study of the project documentation.
- Examination of contracts tests.
- Examination of comments in code.
- Comparison of the desired model obtained during the study with the reversed view obtained during the blind audit.
- Exploits PoC development with the use of such programs as Brownie and Hardhat.

Stage goal

Detect inconsistencies with the desired model.

4. Consolidation of the auditors' interim reports into one:

- Cross check: each auditor reviews the reports of the others.
- Discussion of the issues found by the auditors.
- Issuance of an interim audit report.

Stage goals

- Double-check all the found issues to make sure they are relevant and the determined threat level is correct.
- Provide the Client with an interim report.

5. Bug fixing & re-audit:

- The Client either fixes the issues or provides comments on the issues found by the auditors. Feedback from the Customer must be received on every issue/bug so that the Contractor can assign them a status (either "fixed" or "acknowledged").
- Upon completion of the bug fixing, the auditors double-check each fix and assign it a specific status, providing a proof link to the fix.
- A re-audited report is issued.

Stage goals

- Verify the fixed code version with all the recommendations and its statuses.
- Provide the Client with a re-audited report.

6. Final code verification and issuance of a public audit report:

- The Customer deploys the re-audited source code on the mainnet.
- The Contractor verifies the deployed code with the re-audited version and checks them for compliance.
- If the versions of the code match, the Contractor issues a public audit report.

Stage goals

- Conduct the final check of the code deployed on the mainnet.
- Provide the Customer with a public audit report.

Finding Severity breakdown

All vulnerabilities discovered during the audit are classified based on their potential severity and have the following classification:

Severity	Description
Critical	Bugs leading to assets theft, fund access locking, or any other loss of funds.
High	Bugs that can trigger a contract failure. Further recovery is possible only by manual modification of the contract state or replacement.
Medium	Bugs that can break the intended contract logic or expose it to DoS attacks, but do not cause direct loss funds.
Low	Bugs that do not have a significant immediate impact and could be easily fixed.

Based on the feedback received from the Customer regarding the list of findings discovered by the Contractor, they are assigned the following statuses:

Status	Description
Fixed	Recommended fixes have been made to the project code and no longer affect its security.
Acknowledged	The Customer is aware of the finding. Recommendations for the finding are planned to be resolved in the future.

1.3 Project Overview

The Rubic is a swapping/bridging aggregator supporting several DEX and cross-chain bridges. Most of functionality is implemented as diamond proxy (ERC-2535). Additionally, the project supports after-bridging execution of arbitrary code on some cross-chain bridges.

Rubic implements fees colletion on behalf of some partners (integrators).

1.4 Project Dashboard

Project Summary

Title	Description
Client	Rubic
Project name	Rubic
Timeline	23.02.2023 - 30.03.2023
Number of Auditors	3

Project Log

Date	Commit Hash	Note
22.02.2023	8843336c50ca43e5b5bbe970f17e284f63a96763	initial commit for the audit
22.03.2023	90936a5fbff2959fcb4de5b52274ef724af6c4aa	fixes for the reaudit

Project Scope

The audit covered the following files:

File name	Link
Facets/AccessManagerFacet.sol	AccessManagerFacet.sol
Facets/DexManagerFacet.sol	DexManagerFacet.sol
Facets/DiamondCutFacet.sol	DiamondCutFacet.sol
Facets/DiamondLoupeFacet.sol	DiamondLoupeFacet.sol
Facets/GenericSwapFacet.sol	GenericSwapFacet.sol
Facets/OwnershipFacet.sol	OwnershipFacet.sol
Facets/WithdrawFacet.sol	WithdrawFacet.sol
Facets/GenericCrossChainFacet.sol	GenericCrossChainFacet.sol
Facets/StargateFacet.sol	StargateFacet.sol
Facets/XYFacet.sol	XYFacet.sol
Helpers/ReentrancyGuard.sol	ReentrancyGuard.sol
Helpers/TransferrableOwnership.sol	TransferrableOwnership.sol
Helpers/Validatable.sol	Validatable.sol

File name	Link
Libraries/FullMath.sol	FullMath.sol
Libraries/LibAccess.sol	LibAccess.sol
Libraries/LibAllowList.sol	LibAllowList.sol
Libraries/LibBytes.sol	LibBytes.sol
Libraries/LibDiamond.sol	LibDiamond.sol
Libraries/LibMappings.sol	LibMappings.sol
Libraries/LibUtil.sol	LibUtil.sol
Periphery/ERC20Proxy.sol	ERC20Proxy.sol
Periphery/Executor.sol	Executor.sol
Periphery/Receiver.sol	Receiver.sol
RubicMultiProxy.sol	RubicMultiProxy.sol
Facets/FeesFacet.sol	FeesFacet.sol
Facets/MultichainFacet.sol	MultichainFacet.sol
Facets/SymbiosisFacet.sol	SymbiosisFacet.sol
Helpers/SwapperV2.sol	SwapperV2.sol
Libraries/LibAsset.sol	LibAsset.sol
Libraries/LibSwap.sol	LibSwap.sol
Libraries/LibFees.sol	LibFees.sol

Deployments

Network: Polygon

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0xa5d7797dacd84a0ddf926272f87ea711e73c1024ecccd7d22905521db504be1d
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0xb50c1677d4e9f572ab52e959ab93e768b23f25def2f9d21b7ab755636de8c9aa
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0xd2229f70e18429cdd4b80a16a19010ac3fe5dbc0d757c7facc9534d999c06eca
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0x4afb8240a7c69c3555ca5db3a57b532489e06c24cebcd068cf3611f79b638c43
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0xcf1d22ade17b8311e951da23727eb2169bea7c3aa81a034b09cc8dcb3db509ee
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x7341bd52dc70fb4104760a06712e25a5b6a96ec124db0dba4fabbbcc6e29c69d
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0x9bfa301eba82b8adf08f470f3fc3411a5c9ce812e6884a49e14a4e2d52b2631c
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0x4d2e9287502ed2a611a1670166ab4b7f3af389dba8675296264f71704069b0e0
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0xb1f06b75a8a0e6e7ae90c119fb447adbba865c26c0fa469b79f915e619f40ce9
SymbiosisFacet	0xeCF2e32AfC90A774b0fc3cbd012B681EBfaA0BAF	0xa71f030997626405d1c4f57da79a39265a38c9d2a1dd02d9f76b1eefa53b932d

Contract	Address	Creation TX hash
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0xd01f7734dfa8ad7b87a55c9170c550c31cae174da7583f84dd774f361400e6f9
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0xc31f8730d27ee0a46b880b51a100d9ec7e45407e089a9343aa07ee96739764fe
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0xebee214ddaff5131a7966653aa2f0f61f56c6d448f089fc9b7f902d91a1aeccb
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0xace4da35967ef44395bf9a6596035dd96667d6a16088479f1962c0b311ded757
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0x2f02067441a5eda3fe6f577267c0a663e9d5cd21f3b52b90864ff0bf344eca6d
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0x6c0f250611fbfadb49663590af97c457e45a1d4d9366399b4512bc05b46c3c91
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x5e7a6f446d3109e974e928b1957f9a485d080beeb92d8e55c0103d063bb433e6

Network: Fantom

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x840eb20eecd537073f2175a263d4d045469556fba61c42f51e57dd6eb612237b
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0x87dc42e3cbbe2a7f8fed50ec5db436eecdef4d92243d1a3bafaf75fd0dec00df
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0xb9cf3678583ae8a1eff58785a22cfc84424a44dbed890fbcb3e4c994e3141501

Contract	Address	Creation TX hash
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0x946cdb567f3007df2f9d00d6177aa38e09fe999ab8f872dd5ae7c9824dbf6928
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0xb3c73763df20f886e183e389f37dae941c7ca269efe7e6dea41a72296d06e9eb
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x8ea6d4d40a3f304b8932a45c3d6c456dbde270ca01701ee18033474b8e1a2aff
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0xe28bce50cfca465e4e4f3254cd808e75eac9c9eb31b5a66762ff9289a1168560
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0xa711171200b46f94d2feb6c02387363f328ec49843aa6040f63fefce849bf183
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0x48ca80fe2748a7af01c735d5933eb54024492328cd56147e4763039cca8711c9
SymbiosisFacet	0xeCF2e32AfC90A774b0fc3cbd012B681EBfaA0BAF	0xbdef1f872c76de59c9bf22e3519a4e55ce75b936f6fba2f1dca22343e27f0a16
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0x031997416029cba4e26fe05314415341516333031acb2f53ea7a82f516e66913
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0x7c63e640e788f0dd19a83d6716428c9577bdea65d27ac385d15a2d472815a0b8
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0x3321cc089d2c2056feebcef3300cda912963802c3118a04ff65e6bb8161f39e9
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0x822d52920636281514f0e520f8fd3bd131cc48665ac31d0ce6b954614b525bfe
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0x3e692bdffa3320a3278ba88708e470ac05c5cea3a32d67632ecd474d86238e6b

Contract	Address	Creation TX hash
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0xeeaadc2eb8d6530c3549615a31b61a0cd381d2db33201cf915fe9389e2675597
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x522b26771e2b49bcbdd4433d4bb7227c183a31c56a0a4d977bf116f0e32e5f0e

Network: Cronos

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x740e2540f9cb4d6085cde5bdebd941122db121f6e44b5439683464edbb9b89d3
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0xa99381b1acd95f2a2e63d555ba49d9c888b139446e0ad4f75806e2a61fd53804
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0xf5c483c11779727f54565643c7199af603316dd830f41a34c90b1afb1b902e95
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0xec716702e927bd74c67099ca9b639dff40d92aa30fa8c68f933d8d6fc6563ab2
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x98c5252cb280c5dcaad8b8e114b7c97b737a69d7505cfbb0ce9cd18671eba77e
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0x405c8f6066856278d239caba881057e35531f177182b696a3221860912c3206d
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0xce0b6a1c0c311c84accca0e819760bc31797786c361a69f65fb7cf26359ebe30
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0x111eab608d651c2a8d80cd2379c4dea5f0125c3e8e5e5e612df6f8d2ed5aff7a

Contract	Address	Creation TX hash
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0x9c2c29fa2ef03fcd2b776bbc13148951c6e42926a6dec7196927362024420adf
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0x0c7e79be5da7c061235fb3ee428e32d466faaf84b4a57fba9ecb38582d6edd71
XYFacet	0xAb295d9a639029D7543F7cC5E88594aD8059e63C	0xc7fe2ea676866d23ce83b103a3d98350700521e0579eb8118837957872a699c3
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0x9b5a397b576d797adabcbff2d622e0e3644e8c0ddf90bde3d46e4b44c4ab25d0
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0xd6f42f0f4e9af00703e72fe55f7a0e4cabef3b6d9c22914576c7ba249b44fa20
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0xef1676f002f3794d78a6ee0d8e0eb59665f7441c0f327df0fd30cb5e0cb0dedf
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0xcc5e74f533696b314e7acca6b2b89800252b8e1d0b6ec009eadabf673052c423

Network: Moonriver

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x3c4f337e09911313550a6f1c435ab9f35e351ae332d8ff022f02b5861fa55257
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0x860da17bf4fcd003cbfab076e7d82f744ac88dfea6619c8d0cd2c960e3fbadd7
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0x9329c4d62e7f2f72caaf9b7f112cc36b21efe80a8548a7b4dd0a65f34e9a2b9a

Contract	Address	Creation TX hash
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0xa0bb6020ea7fdde32e0f53e84bdbcca2391227d15a7b8ec6d3de8e611b1fd8d3
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0x4291c9edb7d6460b11052c19a91313628c3f5d905f7e2fd93e683b951ef6fb0a
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x8011f7ec1a6c312536688ee70cf2e4796bc8731f6239dec32f0bd8f938ea0d13
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0xbd507c4d73ef3354cafea6771e8d3f6e96259a1aad1b8068774a287966218c78
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0xd8c080777618a13cf38b5d1c0b6247e89a8ef2e8b8f1df248fcd858220c1c737
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0xd436f70850be9cf067d8eb16fbcf28a7d7ed82bff8e5ecfc526f96b3d16c0f89
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0x3e99249a9098f2d8053bab6c6d5c81aacf6f13175e01ff728edee76e99476b0d
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0x5a002a03bed373fbb6dca4f4d0acad6846a328c0adc4959b3e76185a1aef4a90
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0x3b4e5bfec96322fdcdbf1c575b487eaf039c2fbcdccc8d2449a89c6c6fcdda3c
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0x4fa720299a12a851aa7aa46d3eaa46aa6bc5251b8ea5ebf34f33a6ac42188e58
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0x5e5598848a3227df70ffed7ed18c565d05427b456d24b5e788ab8945cf7c432f
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x240d520af1dccb7970b39749e00182cf07c17c071c33ef809e77309b76906a7e

Network: Optimism

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x875b5a1b4a257bf3117b533c7cd8d50d5f914b5728cc1ad1a234e30e195e6e6b
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0x858a924020c8273dd1b6d013dd5e2516149e27cdfb58879b5911b17e36afe1e4
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0x0b0914eb1f7630ada3f269cb33bd7aed6418f49ff83567a4d1304250eb4e2980
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0x1c2104d609545e2932fe19b6a5eaf58218459d436a9a9aea193a93c1aa430f3f
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0xb9fc4060a523459e51a903a6dc5fd239cff7beefe8ccb1e66ef737dd0f64c491
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x5c5d6a97e01921586d5699857ca51e5faa3ca59547217376bf20ab93e534d694
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0x06c69119810be3b7350736d3180fd8b08180d8ae7c7fd9bdafd3f5557bbb685e
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0x9c13e413922c4737e703e986c4c2317aa3349d6e64d1f2f6f6d3beb0a7e20a50
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0x433064fd361a5de6487297959130784c48ea36326133f2c0380bf6d28b0cdcc8
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0xd453af6beef2c911d8f59e28a714e2f549f0f9491c133db3d3d56840bde7d9b6
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0x07b8c7dc2b92e7f0cd04024429e29fa6d7571b02b6b8af442bcca3e04f760ad1

Contract	Address	Creation TX hash
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0x9ee4388480d8035862c356583e75640a297bea412d04aab423d4758cb97f2150
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0x8f2fcfb5371e3946f60ff86c1e73cb290e50997c84c7f21ce52ac2cb42296dc3
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0x4bf9cc2e0da26bb1efe7d6cde5134226e89818d0110a955cccb9dbf5de7c8313
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0xbc2847589b7fab5eea04c2d929b8a9dbb00237a76604b964889bc7d989baa15b
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x2e67da2242738626870fc01ca5ed76f7ab1992ecfb8164659851f48e91a8e7d1

Network: Arbitrum

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x56bbf4e3e4e62c0c520474cd03cbc447f0b45ba2e26373cad9e0ab7d7c2419b3
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0x6a3ab724de87b6eeaffc9476f3393eb2ec430fd8dd4aad06288f94b1f6f5016f
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0x62556dfb5fdc6a664fdcf95efbec2071252c0f524dafa48a07de283350b12aa7
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0xb4cae67c7e07124098c5eecf3b1bd6f29c5a01178f9649e0a61c2f033f069290
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0xf95d7cc583067de961c8ab57b3f38189c74e503fc90177238191bda15acb0b68

Contract	Address	Creation TX hash
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x9fdf7cf5d63a91cf6deaa1a193cb12edb906a71a250403e3a5ecd039f5150ea0
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0x479d58038fd20a7cd0c7ce5c808539a4209cc8dd9fd51cf75f96f272d3556408
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0x42c9fe99f11f81cda2ccab2202d1a55d1303114d0941d788ab71d84b03927830
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0x7437916b8f773a150d8f6eee39edb290b184af3eec0389020cf07f16454c110d
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0x172fc556f7e14d5c7a83a23dbc88d2f938dc8609e278efed5c557b9e63d21242
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0xcfb67fbcce1f310e25de1ecf2f4ebbe4913b14d6bbddf9f2f23c174eb1615ee7
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0x70cc5c4a92f679e06e2e489d9b450dce62d57e4d41708a1fe84cde90a717abab
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0xffab8e0bf468ecd59f614d4a43394e2cc3fb71202c6c8fc7b794e01f00421e18
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0xcd58ff07029b429c7426dbe8c0091e49285eb26c2847b17a9974ba6ea84f0906
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0xc36d5e26ed9096e973a403f6c4905b41eb2f52c2c7808cdf8271e24bb4cce17e
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x8f459aa8dda449660fa781707667af4b046fc78121ed836be43813ec2413431b

Network: Avalanche

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0xd0e09ba8fcb4f54ea69220e7d723fa2f1c1d360254282e47f5e35cfbedb4c81e
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0x1be5c458d4431570f7b1d5af7c381b635a5f3ba552ca88dc1579ef0f617cffcb
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0xc1ce6894db58a08a9e98d8c12e958c190f2e8473de45c44c667fa7fa367e5c8d
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0xfa21147f64e28a0abeb8e55f39430620f53825c7447088ce605ef770714c8d77
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0x07a09d131b584c2b899da0ab696f5894819b5465135ec7a45a92875d70efebbb
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x0402701b469e4b5f2598c244d1e39f61a118ff5428dbe4490e1ff4718d308027
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0xae61059418f541e3ad40ff0e228729cbcde9f066cb9f26a64fbe652bf23bb119
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0x87f69cd73e4aaaebd128bec78ae1381333e697903a21b69170c0fe5884fa6d6b
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0xde3821067bad94a77d4c32a7ac610e221e0560d164ab85e353ad253693ef845e
SymbiosisFacet	0xeCF2e32AfC90A774b0fc3cbd012B681EBfaA0BAF	0xf7df2b0591829ec3d2e2c9b7762cb9689640d328f625fb244aa1e3376752ee09
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0xdf2e48aa8fd6a4ed5de2c8dbe2e6e6bf5417a1f832cf05c06cdac790a727d666

Contract	Address	Creation TX hash
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0x97b0dc63d9185a01639817e17fe7fa3b7d74121d10d0f0204e03f2160ab00530
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0xc8a889b228783d8fed36beb8ca965f5f9076e323bc6da4f0f346b1cb12f4a54a
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0x91f08bd5bc2332746b3b4e4157e8a51ffa11c504fff5ac915b34f4f073f5781b
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0x43aa412f405ca3e52dcaffde9afc37baaa2726e8c6b7247e9dfdd7189e9a76ab
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0x64f39cd204106d607f7a84bd7bbcc2b41af8130599e34b4170ec13cabb00fa77
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x5fbaae0229946b79685d6e3c7b1ccfd870c1187691b968e545f31c73fe7a74b7

Network: Ethereum

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x0efbf420777b73d55c9a2490492be77eba3066a1555d31b23f9f2cf12bb216b1
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0xe6b2d4b796f0b9d5fc92372c8cd9082d6fc005e5b022cd315c129dfdf55e0a1a
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0xd57b8bbaa26c07e3b194bd0acb53a05ed0ab83851c3c805572dee5d06ec3ddab
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0x03687e64c669422a748e28d2ead9dd8c1e6e20a94e99ac9bc4e4d9bd89b98cec

Contract	Address	Creation TX hash
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0x63f763b9036fcf1209f4480e8d08219ab1a4edb36d39da611864d223fa8f50c5
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0x50fd1ec3fa197ae24c6e8490b58ec85482698c468ad00042967e330e34525d49
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0x51096ed0a717656cb5290222dc46cea0423edc03aa276b47e57ecc26f05cc00e
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0x8afcf83ec08b117d6394c3f1415e3e2f953a6a47e767c4615ff5eea548ebd056
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0xbc5dbb634905a0d52c145bceeb9110831582ee8c558434658f506cea7b0692a8
SymbiosisFacet	0xeCF2e32AfC90A774b0fc3cbd012B681EBfaA0BAF	0x63a62bbfac1f391708643b24269b66f1f50783fe02dcb7667e60a93004503a8d
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0x69164917f06e38a6362bcc865ad8f819844941075a27ada3e5b020a158a13f53
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0x8f47db4a60c07f7d2ee4c54397a341c1fad64d665852bbf4e511eb252bddef21
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0xf5a341b767ee1cabc942d4d9a90c9ba8feaabf2cf2697a3f12a9a6e69c2a70a1
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0x85edb7ffe7e98cdf246651d9a9c0a9b2a3d5488f994db805c57b6b694875f34f
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0xb4dc48584e0269e6ca320e717ca0717d36af38154e5b916fc9b55c6f51dc556e
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0xee403868e7a7fefde7cf305714e2d8c8e0ad97477192fe30900e84bad806c55b

Contract	Address	Creation TX hash
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0xc1c5c5ac25097728f4f7f44438f9a54ff9e1c51f56d53a1ff6e5445759ff6916

Network: BSC

Contract	Address	Creation TX hash
DiamondCutFacet	0xcc64E129D2A80adee32D9bF2BCBecf0E9226Bfa6	0x2b7d682a90434f5c437b7ac89141d077c8d4c68ec1f34c9d6801ac0c5e526534
RubicMultiProxy	0x6AA981bFF95eDfea36Bdae98C26B274FfcafE8d3	0x43fac4135568cb5e2a8fc90f6cb56fad3d34fb7cb29fc9f7d1909f6a62067873
ERC20Proxy	0x3335733c454805df6a77f825f266e136fb4a3333	0xdad2ce4d5f5f30c860a502342f1abd2586b9f43dcdde7928771d5cbf29b5dd23
DiamondLoupeFacet	0x1918B6cE6E7B1E536de210f43382b958dAfDC3B9	0x0cc920b158fe9bbf0f9c4301295e2fe870b9583524f48580e31c4e1e1fbd76ca
WithdrawFacet	0xF67778b8475Fe1D0b6c392899A61CC1846aC77C0	0x567fc1ba79895cbe79a0cd266a1d4b4a25a2d49abca2890d0aa901b118b99ddb
OwnershipFacet	0x1265C279CbB0DF619808B82cb1f47DC46a10E7e9	0xfe0c69d9f6b11244c22abbd75977d645a90288af4a82f30769e54d27ac9fe336
DexManagerFacet	0x0B24e264659B3c903C818170498e093916Ed66AA	0x4ea6a7ff9546c76f8221c1ea058ed30c92896c7187def6abc6de194d6b58f046
AccessManagerFacet	0x65FDD04099a08b362d8ddB7e4a8EF467D464EC1c	0x6d1aa7400b36133b6216695667cbac36806ccda297b6ac3c949f88c6167de015
FeesFacet	0xEA967afBA9E692E4B8dd984A0713FA5E4139993b	0xf9c7c4bf9d668dd4a7cbef845cce67ca3f9886f452f4f1a22d3fed31751181f0

Contract	Address	Creation TX hash
SymbiosisFacet	0xeCF2e32AfC90A774b0fc3cbd012B681EBfaA0BAF	0xf556db663f03c1d891446f92176af974e854f8d77396f10ab7a5a543029a2c46
MultichainFacet	0x25192a562D1d14735a5b3c52432766a6Cd04a841	0xc2f8277d9307aa13b87f5d2a95771361bd0707266e22b1dd5dae1f1448f485be
StargateFacet	0x578b327C89DF0f33995Cb93415E191e7bF942270	0xa1563f46514d5cf5c837b21127185d396ebd4a538e8fd1511163c761a57486b2
XYFacet	0x21998A2E576B62152D64eCFcE9DE2DAAeCDa75D6	0x338ee2543028648ea94056ad3abd5aebbece90ebdd6eb48d985718d000f06152
GenericSwapFacet	0x9149e311B70A7E61CCe4C963CbeFC6bc72746A22	0xfcbd3fe9697f6da5586bd4a131736dbaba32d007ba0024cacaba60f8964d268d
GenericCrossChainFacet	0x51439AdC4d262580F355c450e78662BC80ab35ed	0x520414fe1fb02736b3a78c72f79a8283238041ac949b196256c6b14503ab3d11
Executor	0x9E4B1205291d21eDaB4f710b2905628640e8D0F1	0xb38ba2466683addbd8de409f185e6dd9d98b17c98c616ee1a1974418f4a39149
Receiver	0xb15A66101ac2A6de589dAd1dCbbd7566DCCaB61D	0x821265cbc1126271d48c6e435bdaf27701e8e99a20a9d57ebd21b214d912d95e

1.5 Summary of findings

Severity	# of Findings
Critical	2
High	0
Medium	2
Low	1

ID	Name	Severity	Status
C-1	Incorrect blacklisting of unsafe calls	Critical	Fixed
C-2	Arbitrary calls execution in `Executor` and `GenericCrossChainFacet`	Critical	Fixed
M-1	Unsafe practice of managing a user's ERC20 approve	Medium	Fixed
M-2	The administrator can modify trusted functionality	Medium	Fixed
L-1	Unused logic	Low	Acknowledged

1.6 Conclusion

During the audit process, 2 critical, 2 medium and 1 low severity findings were found and confirmed by the developers. After the revision performed by the developers, 2 critical and 1 medium findings were fixed, 1 medium (medium.2) was demoted to low severity, and low severity findings were acknowledged. The demoted and remaining findings have low severity and do not affect the overall security of the project.

2. FINDINGS REPORT

2.1 Critical

C-1	Incorrect blacklisting of unsafe calls
Severity	Critical
Status	Fixed in aaaee7ae

Description

According to the current design, the users of `Rubic` perform the ERC20 `approve` to the `ERC20Proxy` contract, allowing the ERC20 ERC20Proxy.sol#L40. It is crucially important to disallow any unauthorized calls to this contract, otherwise the user's ERC20 tokens may be spent by an unauthorized party.

The `LibSwap` library implements mechanics to perform an arbitrary call to an arbitrary address. By design, calls to `ERC20Proxy` are LibSwap.sol#L32. However, the blacklisting is set up in the context of `RubicMultiProxy` and will not work in the context of `Executor`, which is also granted a permission to call `ERC20Proxy` for Executor.sol#L174. Therefore, an attacker can force `Executor` to call `ERC20Proxy` (see the Critical.2 finding), perform an unauthorized `transferFrom` and withdraw the ERC20 tokens of any user who gave an ERC20 `approve` to the `Rubic`.

Recommendation

It is recommended to use more fail-safe practices of managing the ERC20 `approve` as described below in the recommendation for the Medium.1 finding. Additionally, it is advised to fix the blacklist issue for the `LibSwap`.

C-2	Arbitrary calls execution in `Executor` and `GenericCrossChainFacet`
Severity	Critical
Status	Fixed in 90936a5f

Description

The `Executor` contract allows the execution of arbitrary calls in the shared context using the `stargate` functionality or directly by calling the Executor.sol#L114 external function.

`GenericCrossChainFacet` also allows the execution of arbitrary calls in the shared context using the GenericCrossChainFacet.sol#L90.

It allows an attacker to setup ERC777 hooks, to provoke blacklisting and do something harmful to the `Executor` and the `Diamond` operationality.

Executing any external calls in the context of the vulnerable contract (`Executor` or `Diamond`) allows an attacker to intercept a transaction of another user and steal ERC777 tokens:

1. Give an approve to the attacker contract from vulnerable contract for a ERC777 token.
2. Set a `transferOnReceive` callback that executes the attacker contract after each transfer to the`Executor` or `Diamond` contract.
3. Some user executes a swap that utilizes the ERC777 token in the end.
4. The attacker contract using the approve (at step 1) drains the vulnerable contract inside the ERC777 callback implementation function.

Recommendation

It is recommended to allow list calls from `Executor` similar to implementation at the facet part of the project. Additionaly, it is recommended to allow list bridges in the `GenericCrossChainFacet`.

2.2 High

Not Found

2.3 Medium

M-1	Unsafe practice of managing a user's ERC20 approve
Severity	Medium
Status	Fixed in aa579352

Description

As it is stated above in the description of the Critical.1 finding, a user's ERC20 tokens can be spent without the user's confirmation. This bad practice reduces the overall project's security by amplifying the impact of other issues. For example, Critical.1 would have a Low severity, and the Medium.2 would be a no issue, if finding Medium.1 is fixed as recommended.

As a general architecture recommendation, this finding is described as a separate item of the report.

Recommendation

It is recommended that every single spending of the user's ERC20 tokens be explicitly signed by the user.

M-2	The administrator can modify trusted functionality
Severity	Medium
Status	Fixed in a9d23cf0

Description

The `DiamondCutFacet` allows the `Owner` to LibDiamond.sol#L93. In combination with the Medium.1 finding, it may lead to users' wallets being drained. Additionaly, the `Owner` is allowed to ERC20Proxy.sol#L27 to the list of trusted contracts.

Recommendation

It is recommended to resolve the Medium.1 finding in order to minimize the impact of the `Owner`'s actions.

2.4 Low

L-1	Unused logic
Severity	Low
Status	Acknowledged

Description

Modifiers SwapperV2.sol#L31 and SwapperV2.sol#L115 use balances differences before and after swaps to calculate leftovers but no any token is supposed to be on the balance before a swap. That's why using just balances is more efficient and simple.

Recommendation

It is recommended to simplify modifiers and use just balances.

2.5 Appendix

1. Monitoring recommendation

The project contains smart contracts that require active monitoring. For these purposes, it is recommended to proceed with developing new monitoring events based on Forta (https://forta.org) with which you can track the following exemplary incidents:

- Unexpected non-zero balance of native assets and/or ERC20 tokens at the following contracts: `Diamond`, `ERC20Proxy`, `Receiver`, `Executor`.
- The following events emitted: `DiamondCut` (the administrator modified the functionality of the `Diamond` contract), `FixedNativeFee`, `TokenFee` (the administrator modified the fee).

3. ABOUT MIXBYTES

MixBytes is a team of blockchain developers, auditors and analysts keen on decentralized systems. We build opensource solutions, smart contracts and blockchain protocols, perform security audits, work on benchmarking and software testing solutions, do research and tech consultancy.

Contacts


https://github.com/mixbytes/audits_public


https://mixbytes.io/


hello@mixbytes.io


https://twitter.com/mixbytes