



Three Sigma

Code Audit



MOR

MOR Morpho Markets Automated Optimized Loops

Disclaimer

Code Audit

MORE Morpho Markets Automated Optimized Loops

Disclaimer

The ensuing audit offers no assertions or assurances about the code's security. It cannot be deemed an adequate judgment of the contract's correctness on its own. The authors of this audit present it solely as an informational exercise, reporting the thorough research involved in the secure development of the intended contracts, and make no material claims or guarantees regarding the contract's post-deployment operation. The authors of this report disclaim all liability for all kinds of potential consequences of the contract's deployment or use. Due to the possibility of human error occurring during the code's manual review process, we advise the client team to commission several independent audits in addition to a public bug bounty program.

00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f
00000020	61 65 36 33 66 37 34 66	63 31 61 36 61 32 34 36	b6f1b3726c1
00000030	65 31 35 61 30 38 39 63	39 33 31 65 38 33 36 35	ae63f7f4639
00000040	30 30 30 30 30 30 30 30	36 38 64 36 31 39 30 30	e15a089c638
00000050	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	00000009820
00000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1e4ba7445bb
00000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	1fee1456376
00000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	5400bfb1bcd
00000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	57233e0e6bc
000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	fff0001d01e
000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	01010000000
000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	00000000000
000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	f2052a01000
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	4104946b538
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	9c726ac91e6
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	16000ae1390
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	7c66fb8be79
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	3c52da73589
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	d4e0a646381
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	e6224947321
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	1e73a823cbf
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	58eacc00000
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	01000000486
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	

Table of Contents

Code Audit

MORE Morpho Markets Automated Optimized Loops

Table of Contents

Disclaimer	3
Summary	7
Scope	9
Methodology	11
Project Dashboard	13
Code Maturity Evaluation	16
Findings	19
3S-MORE-C01	19
3S-MORE-C02	20
3S-MORE-H01	22
3S-MORE-M01	23
3S-MORE-M02	24
3S-MORE-L01	25
3S-MORE-L02	26
3S-MORE-N01	27
3S-MORE-N02	28
3S-MORE-N03	29
3S-MORE-N04	30
3S-MORE-N05	31
3S-MORE-N06	32

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.		
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ		
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.		
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00			
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00			
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ		
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim		
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH		
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin		
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail		
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ		
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ		
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"		
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%		
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M		
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..		
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f		
00000001	30 31 30 30 30 30 30 30	63 31 61 36 61 32 34 36	b6f1b3726c1		
00000002	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639		
00000003	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638		
00000004	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000009820		
00000005	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb		
00000006	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376		
00000007	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd		
00000008	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc		
00000009	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e		
0000000A	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000		
0000000B	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000		
0000000C	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000		
0000000D	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000		
0000000E	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	00000000000		
0000000F	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff		
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff		
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a01000		
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538		
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6		
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390		
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79		
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589		
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381		
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321		
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf		
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc00000		
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486		

Summary

Three Sigma audited MORE in a 3 person days engagement. The audit was conducted from 02-12-2024 to 06-12-2024.

Protocol Description

MORE Optimizer v1 is designed to consume idle liquidity on correlated asset markets on Morpho such as wETH-wstETH in order to execute loops on the collateral asset. The protocol provides amplified yield for passive depositors, while optimizing underlying markets for target utilization, ensuring competitive rates for lenders. The protocol can automatically adjust the number of loops based on market utilization.

000000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.
000000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ
000000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.
000000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
000000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ
000000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim
000000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH
0000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin
0000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail
0000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ
0000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ
0000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö
0000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..
000000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f
000000010	36 66 31 62 33 37 32	63 31 61 36 61 32 34 36	b6f1b3726c1
000000020	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639
000000030	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638
000000040	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000009820
000000050	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb
000000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376
000000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd
000000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc
000000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e
0000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000
0000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000
0000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000
0000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000
0000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	000000000000
0000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff0
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffff
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a01000
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc000000
000000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486

Scope

Filepath	nSLOC
LoopStrategy.sol	676
ProtocolFeeManager.sol	39

Assumptions

OpenZeppelin is considered secure.

000000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.
000000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ
000000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.
000000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
000000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ
000000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim
000000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH
0000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin
0000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail
0000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ
0000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ
0000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"
0000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..
000000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f
000000010	62 33 37 32	63 31 61 36 61 32 34 36	b6f1b3726c1
000000020	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639
000000030	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638
000000040	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000009820
000000050	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb
000000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376
000000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd
000000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc
000000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e
0000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000
0000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000
0000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000
0000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	000000000000
0000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	000000000000
0000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff0
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a01000
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc000000
000000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486

Methodology

Code Audit

MORE Morpho Markets Automated Optimized Loops

Methodology

To begin, we reasoned meticulously about the contract's business logic, checking security-critical features to ensure that there were no gaps in the business logic and/or inconsistencies between the aforementioned logic and the implementation. Second, we thoroughly examined the code for known security flaws and attack vectors. Finally, we discussed the most catastrophic situations with the team and reasoned backwards to ensure they are not reachable in any unintentional form.

Taxonomy

In this audit we report our findings using as a guideline Immunefi's vulnerability taxonomy, which can be found at immunefi.com/severity-updated/. The final classification takes into account the severity, according to the previous link, and likelihood of the exploit. The following table summarizes the general expected classification according to severity and likelihood; however, each issue will be evaluated on a case-by-case basis and may not strictly follow it.

Severity / Likelihood	LOW	MEDIUM	HIGH
NONE	None		
LOW	Low		
MEDIUM	Low	Medium	Medium
HIGH	Medium	High	High
CRITICAL	High	Critical	Critical

00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000000
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..
00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	0100000006f
00000001	30 31 30 30 30 30 30 30	37 32 63 31 61 36 61 32 34 36	b6f1b3726c1
00000002	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639
00000003	35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638
00000004	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000009820
00000005	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	1e4ba7445bb
00000006	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376
00000007	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd
00000008	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc
00000009	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e
0000000A	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000
0000000B	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
0000000C	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
0000000D	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
0000000E	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	00000000000
0000000F	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a01000
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc00000
00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	01000000486

Project Dashboard

Code Audit

MORE Morpho Markets Automated Optimized Loops

Project Dashboard

Application Summary

Name	MORE
Commit	37107cf335b637e1a4af8977a671bed7155dbb18
Language	Solidity
Platform	Ethereum

Engagement Summary

Timeline	02-12-2024 to 06-12-2024
Nº of Auditors	1
Review Time	3 person days

Vulnerability Summary

Issue Classification	Found	Addressed	Acknowledged
Critical	2	2	0
High	1	1	0
Medium	2	1	1
Low	2	1	1

None	6	6	0
------	---	---	---

Category Breakdown

Suggestion	3
Documentation	0
Bug	8
Optimization	0
Good Code Practices	2

Code Audit

MORE Morpho Markets Automated Optimized Loops

Code Maturity Evaluation

Code Maturity Evaluation Guidelines

Category	Evaluation
Access Controls	The use of robust access controls to handle identification and authorization and to ensure safe interactions with the system.
Arithmetic	The proper use of mathematical operations and semantics.
Centralization	The presence of a decentralized governance structure for mitigating insider threats and managing risks posed by contract upgrades
Code Stability	The extent to which the code was altered during the audit.
Upgradeability	The presence of parameterizations of the system that allow modifications after deployment.
Function Composition	The functions are generally small and have clear purposes.
Front-Running	The system's resistance to front-running attacks.
Monitoring	All operations that change the state of the system emit events, making it simple to monitor the state of the system. These events need to be correctly emitted.
Specification	The presence of comprehensive and readable codebase documentation.
Testing and Verification	The presence of robust testing procedures (e.g., unit tests, integration tests, and verification methods) and sufficient test coverage.

Code Maturity Evaluation Results

Category	Evaluation
Access Controls	Satisfactory . The codebase has a strong access control mechanism.
Arithmetic	Satisfactory . No arithmetic errors were found.
Centralization	Moderate . The owner has control over some functionality, but most of the design is decentralized.
Code Stability	Satisfactory . The code was stable during the audit.
Upgradeability	Satisfactory . The contracts are upgradeable.
Function Composition	Satisfactory . Functionality is well split into helper functions.
Front-Running	Satisfactory . No front-running issues were found.
Monitoring	Satisfactory . Events were correctly emitted.
Specification	Satisfactory . In-depth and well structured high-level specification as well as codebase documentation.
Testing and Verification	Satisfactory . Extensive test code coverage as well as usage of tools and different test methods.

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000001	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000002	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	00000003	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	00000004	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	00000005	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	00000006	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00000007	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	00000008	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	00000009	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	0000000A	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	0000000B	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	0000000C	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	0000000D	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	0000000E	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	0000000F	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	00000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	00000001	66 31 62 33 37 32	63 31 61 36 61 32 34 36	00000002	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	00000003	35 61 30 38 39 63	36 38 64 36 31 39 30 30	00000004	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000005	31 65 34 62 61 37 34 34	62 62 62 65 36 38 30 65	00000006	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	00000007	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	00000008	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	00000009	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	0000000A	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	0000000B	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	0000000C	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	0000000D	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	0000000E	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	0000000F	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	00000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38
----------	-------------------------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	----------------	----------	-------------------------	-------------------------	----------	-------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------------	----------	-------------------------	-------------------	----------	-------------------------	-------------------------

Findings

Code Audit

MORE Morpho Markets Automated Optimized Loops

Findings

3S-MORE-C01

Funds may be stolen by calling **onMoreFlashLoan()** directly

Id	3S-MORE-C01
Classification	Critical
Severity	Critical
Likelihood	High
Category	Bug
Status	Addressed in #7d71809 .

Description

LoopStrategy::onMoreFlashLoan() does not validate that the caller is the market, which allows attackers to steal collateral by calling it directly.

Recommendation

Revert if the caller is not **markets**.

3S-MORE-C02

Malicious **path** can be passed to **redeem/withdraw()** allowing an attacker to draining the strategy

Id	3S-MORE-C02
Classification	Critical
Severity	Critical
Likelihood	High
Category	Bug
Status	Addressed in #ef31c48 , #d9a89a9 .

Description

path is not validated in **redeem/withdraw()**, which could lead to problems as the flow should always sell and buy the same token.

Note: if a reentrant token is passed in the path it may be possible to deposit in the **LoopStrategy** while swapping, which would lead to stolen funds as the ratio would be higher due to having burned the shares but the assets are still in the strategy.

Note2: if **ankrFlow** is reentrant it could also be used to drain the funds.

For example, consider this path:

- attacker creates a pool of wFlow/reentrantToken and ankrFlow/reentrantToken;
 - attacker deposits large amount of funds in the **LoopStrategy**;
 - attacker withdraws using the following path:
 - ankrFlow → reentrantToken
 - reentrantToken → wFlow;
 - whilst swapping, the reentrantToken allows the attacker to reenter the strategy and deposit. This deposit will give inflated shares as the **_withdraw()** method burns the shares first, but only withdraws all the assets by the end (the vault, for example);
 - the attacker withdraws the inflated shares for much more funds.
-

Recommendation

Do not allow arbitrary paths.

3S-MORE-H01

Market interest is not always accrued

Id	3S-MORE-H01
Classification	High
Severity	High
Likelihood	High
Category	Bug
Status	Addressed in #18ede5e .

Description

The **market** accrues interest, which changes **totalAssets()** in the **LoopStrategy**. Thus, everytime there is some action that modifies the amount of assets, interest should always be accrued first. However, **markets.accrueInterest()** is only called on **_withdraw()**, post shares/assets calculation, which will lead to an incorrect asset withdrawal.

On deposit/mint, it also does not accrue market interest before calculating the shares to receive.

In the view functions, such as **totalAssets()**, **expectedAmountsToWithdraw()** or **maxWithdraw()**, it also does not consider the accrued interest from the market.

Recommendation

Accrue market interest before each action and ideally find a way to fetch the accrued interest in a view function (the market does not seem to have this ability currently).

3S-MORE-M01

Vault cap is not considered in the **maxDeposit()** calculations, which may make deposits fail

Id	3S-MORE-M01
Classification	Medium
Severity	Medium
Likelihood	Medium
Category	Bug
Status	Addressed in #4793c1c .

Description

LoopStrategy::maxDeposit() does not consider the vault cap, which limits the amount that can be deposited if the utilization rate is close to the **targetUtilization**. Hence, deposits will revert.

Recommendation

Consider incorporating the **maxDeposit()** of the vault.

3S-MORE-M02

LoopStrategy is vulnerable to inflation attacks

Id	3S-MORE-M02
Classification	Medium
Severity	High
Likelihood	Low
Category	Bug
Status	Acknowledged.

Description

LoopStrategy inherits **ERC4626Upgradeable**, which calculates shares deposited as (`_decimalsOffset()` is 0):

```
shares = assets * (totalSupply() + 1) / (totalAssets() + 1);
```

As such, the following attack is possible:

- User deposits $1e18$ assets.
- Attacker frontruns and deposits 1 asset, minting $1 * 1 / 1 = 1$ share.
- Attacker donates **2e18** worth of vault shares to the market.
- User1 deposits $1e18$ assets and receives no shares, **shares** = $1e18 * 2 / (2e18 + 1) = 0$.
- User2 deposits $1.5e18$ assets and receives no shares, **shares** = $1.5e18 * 2 / (3e18 + 1) = 0$.
- Attacker redeems $1 * (4.5e18 + 1) / (1+1) = 2.25e18$.

Recommendation

Consider using a bigger decimals offset or do an initial deposit.

3S-MORE-L01

In case of high **ltv** and unfavourable swap, **onMoreFlashLoan()** may underflow

Id	3S-MORE-L01
Classification	Low
Severity	Low
Likelihood	
Category	Bug
Status	Acknowledged.

Description

LoopStrategy::onMoreFlashLoan() underflows when **cost** > **collateralToWithdraw**, which may happen in case the market has a high **ltv** and significant slippage occurs.

Recommendation

Consider using the **wFlow** from the **vault** in this case.

3S-MORE-L02

LoopStrategy::totalAssets() tracks the **wFlow** balance, but this is not redeemable

Id	3S-MORE-L02
Classification	Low
Severity	Low
Likelihood	Low
Category	Bug
Status	Addressed in #bc94096 .

Description

The **LoopStrategy** is not supposed to hold **wFlow** directly, but this is still tracked in **totalAssets()**. However, this is not redeemed in **_withdraw()**, so it will be stuck.

Recommendation

Consider withdrawing **wFlow** on **_withdraw()** or remove the balance from the **totalAssets()** calculation.

3S-MORE-N01

In `LoopStrategy::withdraw()`, `_updateLastTotalAssets()` is called after `_withdraw()`

Id	3S-MORE-N01
Classification	None
Category	Bug
Status	Addressed in #c4b4f1a .

Description

In `LoopStrategy::withdraw()`, `_updateLastTotalAssets()` is called after `_withdraw()`.

Recommendation

Follow the CEI pattern and update the total assets before the `_withdraw()` call.

3S-MORE-N02

› should be used instead of != in **LoopStrategy::_deposit()**

Id	3S-MORE-N02
Classification	None
Category	Suggestion
Status	Addressed in #a1ae67f .

Description

LoopStrategy::_deposit() stops iterating if the utilization ratio reaches exactly the target, that is, **market.totalSupplyAssets.wMulDown(targetUtilization) == totalBorrowAssets**. However, if the utilization is bigger, it continues.

Recommendation

This should not be possible given the rest of the function, but using › is more correct.

3S-MORE-N03

Typo in `LoopStrategy::_maxDeposit()`

Id	3S-MORE-N03
Classification	None
Category	Good Code Practices
Status	Addressed in #40132e8 .

Description

`LoopStrategy::_maxDeposit()` has as a comment `totolSuppliable`, which has a typo.

Recommendation

Replace `totolSuppliable` with `totalSuppliable`.

3S-MORE-N04

Approval is not reset to 0 after approving the **markets** for **wFlow** assets repayment in **LoopStrategy::onMoreFlashLoan()**

Id	3S-MORE-N04
Classification	None
Category	Suggestion
Status	Addressed in #f17f609 .

Description

LoopStrategy::onMoreFlashLoan() does not reset the approval of the **markets** to 0 after approving the repayment of **wFlow**.

Recommendation

This is not a problem for **wFlow**, but some tokens revert when approving from a null amount to a non null amount, so consider resetting the approval.

3S-MORE-N05

safeApprove() should be used instead of **approve()**

Id	3S-MORE-N05
Classification	None
Category	Suggestion
Status	Addressed in #72adb3b .

Description

Some tokens do not return a bool on approval, so **safeApprove()** should be used.

Recommendation

Consider replacing all instances of **approve()** by **safeApprove()**. Can be kept as is as the current tokens work without issues.

3S-MORE-N06

paramsOfTheMarket is unused in the **LoopStrategy**

Id	3S-MORE-N06
Classification	None
Category	Good Code Practices
Status	Addressed in #50a9248 .

Description

paramsOfTheMarket is [unused](#) in the **LoopStrategy**.

Recommendation

Remove or deprecate the variable (comment or rename it).