										l libility Count
CLIS Zhanks LeHessenings							Count		2 N = N N N N P P P P P P P P P P P P P P	Function Name Without etablishment of the control of claim of o
3							Severity	Total ligh-Severity losses Total Low-Severity losses Total Low-Severity losses		Type Integer Arthreete Bug Dependence on predeable ever formers a state Dependence on predeable Dependence on predeable ever formers Dependence on predeable
headra-244/674284 AFFX7execution-time \$600 vs. msexecution-time \$300	Project Dashboard	Organ Dollar Soldday Efercan Mythril	Dec 2022 - Jan 2023 Whitebox 2 person	Vulnerable Contracts 2 2 2 12	16 Vulnerabilitis 2 6 5 31 39	Vulnerrability Type Describes a profession or window 1 Describes a profession or window All Manday Calls in study Transaction 2 All Manday Calls in study Transaction 2 All Manday Calls in study Transaction 2 See according to the Call of the		Total	Total Total Total One Watto	Exocution Summary Contract Name Contract Name Inch Conposition/Lima Low Disper
	hounded to dight it gight. Though at it, and fails in set de absociate to be such his data but dight set to deport in an in the second and	America or a signification of the state of t	Indiana Control of the Control of th	International Control of the Control		December 2004 2004	Prof.	1-1	17-0	Total

															ous miner. Also attacker knows the hash of earlier blocks.				rute miner. Also attacker knows the hash of earlier blocks.	Ta prior call fails permanently. This might be caused intentionally by a malicious callee.								f a prior call falk normanouth. This midd be caused intentionally by a malicious called					us mirer. Also attacker knows the hish of earlier blocks.							
														*	values of variables like coimbace, gaslimit, block number, timestamp are predictable and can be manipulated by malicious miner. Also attacker knows the hash of earlier blocks				values of variables like combuse, gadimit, block number, timestump are predictable and can be manipulated by malicious miner. Also attacker knows the hash of earlier blocks,	This call is executed following another call within the same transaction. It is possible that the call never gots executed if a prior call fails permanently. This might be caused intentionally by a malicious callee	assertion voltation							The cell corrected following another cell within the came transaction. It is receible fait the cell near eac account if a mire cell fit is more than the cell near each another cell fit is not interested in the cell near each another cell fit.		sessanting voltation	I RODALINA LA CATROLIA		values of variables like coimbase, gastimit, block number, timestamp are predictable and can be manipulated by malicious miner. Also attacker knows the lasts of earlier blocks							
											Function Name Description			Overflow/ Underflow							gasprice_bit_ether(int128) transfer(address, uint256) many_msg_babbuge(tyks1) Possible to trigger an assertion voilation									X90.3983.9c xx30.23.4db xx20.23.4db xx20.23.4dcb xx20.23.										
											Туре			Integer Arthmetic Bug ethUsdPrice() Denombrace on predictable claim()	environment variablefunction_0x3b650d29			Dependence on predictable function 0x73796297		Multiple Calls in a [function_0] single Transaction	gasprice_bit transfer(addi many_msg_							Multiple Calls in a sincle Transaction (1x02)8s477		Innetion (0x06) 3839e Innetion (0x06) 2346b Innetion (0x07) about			Dependence on predictable environment variablefunction_0x73796297							
											red Severity	20		E High	E	ш	m		E Low	E Low	Medium			В						Medium		В	E Low	m m				2 2	m m	
gasprice_bit_ether(int128) transfer(address, uint256) many_msg_babbage(bytes 3	function_0x0a28a477 1	function 0x9b39839e function 0xe3b23d6b function 0xf92ebsac 3		unction_cots/fract3 unction_cots/fract3 unction_cot/fract31b 4	_function_cx+97/dect3 _function_cx+92/dest28 _function_cx7/dest283b _function_cx7/95/2914 4		function_0xc32c7202 1	and the search of the search o	Imention 0x2376dff 8 function 0x1516df8 8 function_0x00486499 1		Result Terminal Output Deployed 0 TRUE	at definition of the party of the second of the second	-	TRUE		100	ton		TRUE	TRUE		_		0 TRUE	0 TRUE	and the state of t	· · · · · · · · · · · · · · · · · · ·	U TRUE		Market and the second s		0 TRUE		0 TRUE			0 TRL		TRUE	TRU
	Multiple Calls in a single Transaction		Dependence on predictable environment variable	Multiple Calls in a Single Transaction	Multiple Calls in a Single Transaction	d de la company			External Call To User-Supplied Address Integer Arithmetic Bugs		ByteCode																							9B69917F96001712Ad5 9992dr74F1DA55e60a19	0422ft2C4FDbb2B32 aAD1cA0ac27f777a90	73995cC990697af1B8 11Db9aD85a38Aa264cb3	0690D965C120226689	8BB9D37346d0726c09		
Medium	Low	Medium		Low	Low		Low S		Low			0x5e3646A1Db86993F3E6b 74AS7D8640B69F7e2S9	0x6C5cdfB471S0EFe52072c B93Eca1e0F123529748	0x017aD99900b9581Cd40C 815990890EE9F0858246 0x9C944f04504BA1-ab94430	C006c269C314B1A8281 0x2A8cl E676Ec238d8A992	3(7B495b45B3fEAa5e86 0x9c459eeb3FA179a4(B29b	81C1635525e9A0Ef094 0xB6764c2Cc8F1IDCd89AF	1C3e246f886579746233 0xe7068A3SF9F5b7747IBe	FfBdf82D9531D52AFCde	0xcecaD 69d7D4Ed6D52eFc FA028aF8732F27e68F70	0 xeecaD 69 d7D 4Ed6 D52eFe FA028 aF 8732 F27c48 F71	0xcecaD 6947D4Ed6D52eFc FA028aF8732F27e08F72	0xcecaD 69 d7D 4Ed6 D52eFe FA0 28aF 8732 F2 7c08 F73	0x72426BA137DEC6265730 6b12B1E869d43FeC6eC7	0x5 E72EB0ab74B5B4d2766 a7956D210746Ccab96E1	0.5.3db8d52d65F75E4cdDA 1b02463760e9561A2aa1 0.5.2BEBd3d7f37EC428485	3Fd5861Ac71253A7F428 0xD2a830E8CBdFed6CC1	1 Bab697bB25496cd6FA62 0xBF3B9b141Cb3629F5Bb 8F7214A 9765-02304530	0xC72bda59E382be10bb5D 71aBd01Ecc65aa16D83	0x845330DC8005e13dEA30	TOTAL CONTROL OF THE	0xEEcD72c99749A1FC9777 04AB900a05c8300F4318	0x80C898ac5e56R8836E2 35CeB8CEa3EB726CB58	0 xC 69 TEab7 B9F Sc5 cEZd35 B9B6 99 17 F9 600 17 12 Ad5 0 x7 A1 92D D9 Cc4 Ea0 bdEdeC 99 92 df74 F1 DA5 Sc6 0a 19	0xc7faB3de576caf6044369930422f12C4FDbb2B32 0x89Eb88fEde50FC77ae8a18aAD1cA0ac27f777a90	0 xEx83F8eBB435373 f6x21 1173995cC990 697 aft B8 0 xEx2 Effect25x4749D4A6 f041 D49a185a38 Aa2 64cb3	0.2.1 F F 81 2D 70 B 33 96 880 D 3 0 9 0 D 9 5 C 1 2 0 2 0 5 6 6 8 9 9 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0x79F2188EF9550A1 dCT1A 062cca 0a bE9068450197 0x5 cC70898c47f732.65BdE5b8BB91x37346d072.6c09		
5 Flipper	6 WrappedOusd	7 MixOracle	8 DripperProxy	9 Properties/OUSD Trans ferable	10 TestOUSDTransferable	11 T from Edition December	12 MeckRewardPool	14 Mock-Awel neem (west-Control let	15 Mock NonRebasing 16 Mock UniSwapRouter	Complete OUSD Execution	Contract Name	2 AaveStrategyProxy	3 Buyback	4 ChainlinkOracle	5 CompensationClaims	6 InitializeGovernedUpgradeabilityProxy	7 CompundStrategyProxy	8 Convex Generalized MetaStrategy	9 Dripper	10 Flipper	11 Flipper	12 Flipper	13 Flipper	14 Governor	15 Harvestor	16 OUSD	17 MinuteTimeLock	18 WrappedOUSDProxy	20 Mombo Aave Stratery		22	23 Vaul ValueChecker	24 DripperProxy	25 CompoundStrategy 26 Convex LUSDMetaStrategyProxy	27 ConvexOUSDMetaStrategy 28 ConvexOUSDMetaStrategyProxy		31 HarvesterProxy	32 Morpho CompoundStrategy 33 Morpho CompoundStrategy	34 MorphoCompoundStrategyProxy 35 OGNStakingProxy	36 OUSDReset

y. This might be caused intentionally by a maticious callee.	r. This maiste has contract interestionally that a multicious colline	 Ins mgm be caused intentionally by a maticious callee. 				vs the hash of earlier blocks.																		nitact in an infermediate state.		ntract in an intermediate state.	lees can be trusted (i.e. they're part of your own codebase).							ted after this call and/or recenturey gasted are in plece.								
The call is exected following another call white the same transaction. It is possible that the call never gos executed if a prior call this permanenty. This might be caused internationally by a makebout callect	This call is a considered for the miner and when the same tens retired it is a considered for a circumfactor to	I INS CALLI SENCENCIAL UNIDIDIDIDIDIDI DE SIMPE GRANGE GRANGE CARLO CALLO CALL				values of variables like coimbase, gaslimit, block number, timestamp are predictable and can be manipulated by malicious miner. Also attacker knows the hash of earlier blocks																	1	before the call, especially if the callee is untribled. Alternatively, a reentrancy lock can be used to prevent untribled callees from re-entering the contract in an informediate state.		before the call, especially if the calbe is unmasted. Alternatively, a reentrancy tock can be used to prevent untrusted calbes from re-entering the contract in an intermediate state.	directionally by a malixious callee. If possible, refactor the code such that each transaction only executes one external call or make sure that all call;							in this contact. Recented is an intermediate state may bad to unexposed behaviour. Make sure that no state medifications are executed they this call and/or recentracy garand are in place						Overflow Underflow		
function 0x197decf3 function 0x400f42f function 0x7daa2a3b function 0x7f502914	function_0x197dccf3 function_0x80f92F function_0x7dsa2a3b function_0x78x02018	Tunction_0x/t5/02914			Innetion_Oxbec39x6b function_Oxbec39x6b function_Oxbec39x8b function_Oxbbcybce function_Oxbbcybce	nclaim()																		_tunction_0xc52e7202			x_function_0x3111e7b3							_function_0x1caa8781 inproved fordabless usin256) increases Allowsunced dates usin256 increases Allowsunced dates usin256 intransfer and any map, abulled polytes 11 transfer dates usin256 intraction_0x1510681 interaction_0x23564ff and increases_0x23564ff and increases_0x23564ff and increases_0x23564ff and increases_0x235106164						_function_0xc04b8d59 _function_0xc04b8d59		
Multiple Calls in a Single Transacti	Mathiala Calle in a Simula Transmoti	Munipe Calis in a Single Transact			Interior Ovec3940 Interior Ovec3940 Interior Ovec3940 Interior Over889841 Interior Over1970 Interior Over1970	Dependence on predictable environ																		State access after external call		State access after external call	Multiple Calls in a Single Transacts							External Call To User-Supplied Add						Integer Arithmetic Bugs		
TRUE Low	HIGH	TRUE	TRUE	TRUE	TRUE	TRUE Low	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE Low	TRUE	TRUE Low	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE Loss		HIGH	TRUE	TRUE	TRUE	TRUE High	TRUE	TRUE
		0	0	0	0	The second secon	0 0	0	0	0 0	0	0	0 0	0	0	0	0	0	0	0	0	Table 1 Company of the Company of th	0	0	0		0	0	0	0	0	0	0 0			0 0		0	0	To the state of th	0	0
0x.6080.64-00.05.20.00.05.20.00.05.00.00.00.00.00.00.00.00.00.00.00	An-COUNTY MONTH TO THAT ACT AND ACT AN	CX 60 80 60 40 525 48 0 1 0 0 1 52 1 0 8 1 57 1 0 6 1 0 6 1 0 7 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0x60806040523480156100105760080fd5560000	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 fd5b5 06 004	HONOR CHECK LINGUISTICS OF THE BOTH THE	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 fd5b 5 06 004	0x60306040052248015610010576000301d25506004 0x6080604052248015610010576000301d25506004	0x6080604052348015610010576000807d5b506004	0x 6080 60 40 523 48 01 56 10 01 05 760 0080 fd5b5 06 004	0x 60 80 60 40 526 00 43 61 06 10 20 457 60 00 35 60 e01 c80 0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 61515 06 00 4	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 fd5b 5 06 004	0x608060405234801561001057600080fd5b506004	0x 60 80 60 40 525 48 01 56 10 01 05 760 00 801 d 55 50 60 10 4 0x 60 80 55 60 60 1 c 80	0x6080604052600436106100865760003560e01e80	0x 60 80 60 40 526 00 43 61 06 10 08 657 60 00 35 60 e01 c80	0x6080604052348015610010576000801d5b506004	$0 \times 608060405234801561001057600080fd.55506004$	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 1455 56 004	0x6080604052348015610010576000801d50506004	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 fd 50 5 06 004	0x608060405234801561001057600080105506004	0x 60 80 60 40 522 48 01 56 10 01 05 760 00 80 1d 55 56 004	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 fd5b 5 06 004	0x60306040052248015610010576000301d25506004 0x6080604052248015610010576000301d25506004	0x608060405234801561001057600080fd5b506004	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 fd5b 5 06 004	0x 60 80 60 40 523 48 01 56 10 01 05 760 00 80 6450 50 600 40 x 60 80 64 40 523 48 01 56 10 01 05 760 00 80 6450 50 600 4	0x608060405234801561001057600080fd5b506004	0x 6080 60 40 523 48 01 56 10 01 05 760 00 80 fd5b5 06 004	0x 60 80 60 40 522 48 91 56 10 01 05 760 00 80 1150 5 06 004 0x 60 80 60 40 523 48 91 56 10 01 05 760 00 80 1150 5 06 004	0x608060405234801561001057600080fd5b506004	0x60806040523480156100105760080fd5b506004	0x 60 80 60 40 522 48 01 56 1001 05 760 00 80 10 50 50 00 00 00 760 00 80 10 50 50 60 00	- 0x-c000 c0 152 t0 01 157 10 00 157 00 00 00 00 00 00 00 00 00 00 00 00 00	THE	0X 60 80 C C C D C C C C C C C C C C C C C C C	0x 48 88 46 48 526 88 43 64 8 425 57 66 88 35 68 68 108	0x6080604052348015610010576000804050	0x60896646523488156190195766988645556984	0x 68 86 68 46 526 99 43 61 96 18 955 57 68 98 35 69 e8 1 c8 (0×7300000000000000000000000000000000000	0x73 00 00 00 00 00 00 00 00 00 00 00 00 00
38 PropertiesOUSD Trans ferable	2.0 ToolOlistYTenneloonkla	40 Grammable	41 InitializableGovernable	42 Strategizable	45 Vali	44 LiquidityReward	45 SingleAssetStaking 46 OttoleRouter	47 OnseleRouterDev	48 VaultAdmin	49 VanitCore 50 Vanithinitalizer	51 VaultStorage	52 OUSDRescoultionUpgrade	55 Timekock 54 OUSDPoxy	55 ThreePoolStrategyProxy	56 VaultProxy 52 Mo-t-2/DV	58 MockBooster	59 MockCRV	60 Mock Deposit Token	62 MockCurveGuage	63 MockCurveLUSDMetapool	64 MockCurveMetapool	66 MockCVX	67 MockLUSD	68 Mock Reward Pool	70 Mock/Token	71 Mock AaveIncentivesController	Mock Aave Incentives Controller 72 Mock AAVE Token	73 MockChainlinkOracleFood	74 MockCOMP	76 MockCroken	77 MockDA1	78 MockEvilDAI	79 Mock Limited Wrapped Cuiso 80 Mock Minsble Uniswan Pair	S) Mock-build-basing.	MATERIAL PROPERTY OF THE PROPE	82 Mock NonStandard loken 83 Mock WFTH	84 Mosk Vault	88 MockUSDT	86 MockUSDC	87 Mock UniSwapRouter	88 Helpers	89 StableMath