## // HALBORN

## Affine DeFi -Multiplyr Smart Contract Security Audit

Prepared by: Halborn Date of Engagement: September 19th, 2022 - October 7th, 2022 Visit: Halborn.com

DOCL	DOCUMENT REVISION HISTORY		
CONT	TACTS	4	
1	EXECUTIVE OVERVIEW	6	
1.1	INTRODUCTION	7	
1.2	AUDIT SUMMARY	7	
1.3	TEST APPROACH & METHODOLOGY	7	
	RISK METHODOLOGY	8	
1.4	SCOPE	10	
2	ASSESSMENT SUMMARY & FINDINGS OVERVIEW	12	
3	FINDINGS & TECH DETAILS	13	
3.1	(HAL-01) IGNORE EXTERNAL CALL FEE - MEDIUM	15	
	Description	15	
	Code Location	15	
	Proof of Concept	16	
	Risk Level	17	
	Recommendation	17	
	Remediation Plan	17	
3.2	(HAL-02) POSSIBLE LOSS OF FUNDS - MEDIUM	18	
	Description	18	
	Code Location	18	
	Proof of Concept	18	
	Risk Level	19	
	Recommendation	19	
	Remediation Plan	19	

3.3	(HAL-03) POSSIBLE UNPREDICTABILITY BETWEEN L2 AND L1 RATIOS	6 - 20
	Description	20
	Code Location	20
	Risk Level	20
	Recommendation	20
	Remediation Plan	20
3.4	(HAL-04) FUNCTION DOES NOT CHECK THE TOKEN BALANCE BEFORE A	AND 21
	Description	21
	Code Location	21
	Risk Level	21
	Recommendation	22
	Remediation Plan	22
3.5	(HAL-05) LACK OF PROPER SLIPPAGE PROTECTION - INFORMATIONAL 23	_ }
	Description	23
	Code Location	23
	Risk Level	23
	Recommendation	23
	Remediation Plan	24
3.6	(HAL-06) POSSIBLE MISUSE OF CHAIN ID - INFORMATIONAL	25
	Description	25
	Code Location	25
	Risk Level	25
	Recommendation	26
	Remediation Plan	26

4	AUTOMATED TESTING	27
4.1	STATIC ANALYSIS REPORT	28
	Description	28
	Slither results	28
4.2	AUTOMATED SECURITY SCAN	47
	Description	47
	MythX results	47

## DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	10/04/2022	Omar Alshaeb
0.2	Draft Review	10/07/2022	Kubilay Onur Gungor
0.3	Draft Review	10/07/2022	Gabi Urrutia
1.0	Remediation Plan	10/26/2022	Omar Alshaeb
1.1	Remediation Plan Review	10/28/2022	Kubilay Onur Gungor
1.2	Remediation Plan Review	10/28/2022	Gabi Urrutia

CONTA	CTS	
CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Kubilay Onur Gungor	Halborn	Kubilay.Gungor@halborn.com

Omar Alshaeb	Halborn	Omar.Alshaeb@halborn.com

# EXECUTIVE OVERVIEW

### 1.1 INTRODUCTION

Affine DeFi engaged Halborn to conduct a security audit on their smart contracts beginning on September 19th, 2022 and ending on October 7th, 2022. The security assessment was scoped to the smart contracts provided to the Halborn team.

### 1.2 AUDIT SUMMARY

The team at Halborn was provided three weeks for the engagement and assigned a full-time security engineer to audit the security of the smart contract. The security engineer is a blockchain and smart-contract security expert with advanced penetration testing, smart-contract hacking, and deep knowledge of multiple blockchain protocols.

The purpose of this audit is to:

- Ensure that smart contract functions operate as intended
- Identify potential security issues with the smart contracts

In summary, Halborn identified some security risks that were mostly addressed by the Affine DeFi team.

### 1.3 TEST APPROACH & METHODOLOGY

Halborn performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of this audit. While manual testing is recommended to uncover flaws in logic, process, and implementation; automated testing techniques help enhance coverage of the bridge code and can quickly identify items that do not follow security best practices. The following phases and associated tools were used throughout the term of the audit:

- Research into architecture and purpose
- Smart contract manual code review and walkthrough
- Graphing out functionality and contract logic/connectivity/functions (solgraph)
- Manual assessment of use and safety for the critical Solidity variables and functions in scope to identify any arithmetic related vulnerability classes
- Manual testing by custom scripts
- Scanning of solidity files for vulnerabilities, security hotspots or bugs. (MythX)
- Static Analysis of security for scoped contract, and imported functions. (Slither)
- Testnet deployment (Brownie, Remix IDE)

### RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

### RISK SCALE - LIKELIHOOD

- 5 Almost certain an incident will occur.
- 4 High probability of an incident occurring.
- 3 Potential of a security incident in the long term.
- 2 Low probability of an incident occurring.
- 1 Very unlikely issue will cause an incident.

#### RISK SCALE - IMPACT

- 5 May cause devastating and unrecoverable impact or loss.
- 4 May cause a significant level of impact or loss.

- 3 May cause a partial impact or loss to many.
- 2 May cause temporary impact or loss.
- 1 May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
10 - CRITICAL 9 - 8 - HIGH 7 - 6 - MEDIUM 5 - 4 - LOW 3 - 1 - VERY LO		ΓIONAL		

### 1.4 SCOPE

IN-SCOPE:

The security assessment was scoped to the following smart contracts:

- src/ethereum/L1CompoundStrategy.sol
- src/ethereum/L1Vault.sol
- src/ethereum/L1WormholeRouter.sol
- src/external/Multicall.sol
- src/interfaces/\*
- src/polygon/Detailed.sol
- src/polygon/EmergencyWithdrawalQueue.sol
- src/polygon/ERC4626Router.sol
- src/polygon/ERC4626RouterBase.sol
- src/polygon/Forwarder.sol
- src/polygon/L2AAVEStrategy.sol
- src/polygon/L2Vault.sol
- src/polygon/L2WormholeRouter.sol
- src/polygon/Router.sol
- src/polygon/TwoAssetBasket.sol
- src/AffineGovernable.sol
- src/BaseStrategy.sol
- src/BaseVault.sol
- src/BridgeEscrow.sol
- src/Constants.sol
- src/DollarMath.sol
- src/WormholeRouter.sol

Commit ID: 30e93568ca0b0b458f8744bae1e62aaf1e132647

And the following smart contracts:

- src/ethereum/CurveStrategy.sol
- src/ethereum/ConvexStrategy.sol
- src/polygon/DeltaNeutralLp.sol

Commit ID: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

Fixed Commit ID: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

And the following smart contracts:

- src/BaseVault.sol
- src/ethereum/L1Vault.sol
- src/polygon/L2Vault.sol

Commit ID: 302ab4e2e54c2666d607be1b88861636fdee311d

## 2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	0	2	2	2

### LIKELIHOOD

	(HAL-01) (HAL-02)			
-				
		(HAL-03)		
		(HAL-04)		
	(HAL-05) (HAL-06)			

IMPACT

EXECUTIVE OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
HALØ1 – IGNORE EXTERNAL CALL FEE	Medium	SOLVED - 10/26/2022
HALØ2 – POSSIBLE LOSS OF FUNDS	Medium	SOLVED - 10/26/2022
HAL03 - POSSIBLE UNPREDICTABILITY BETWEEN L2 AND L1 RATIOS	Low	RISK ACCEPTED
HAL04 – FUNCTION DOES NOT CHECK THE TOKEN BALANCE BEFORE AND AFTER A CALL	Low	SOLVED - 10/26/2022
HAL05 - LACK OF PROPER SLIPPAGE PROTECTION	Informational	SOLVED - 10/26/2022
HAL06 - POSSIBLE MISUSE OF CHAIN ID	Informational	SOLVED - 10/26/2022

# FINDINGS & TECH DETAILS

### 3.1 (HAL-01) IGNORE EXTERNAL CALL FEE - MEDIUM

Description:

The wormhole publishMessage function is payable. Currently, requires no fees, but that can be changed over time. If the wormhole decides to set a fee greater than 0, all those external calls within the protocol would fail. Hence, leaving the wormhole routers unable to perform their critical tasks.

Code Location:

Listing 1: L2WormholeRouter.sol (Line 33)
29 function reportTransferredFund(uint256 amount) external {
30 require(msg.sender == address(vault), "Only vault");
31 bytes memory payload = abi.encode(Constants.
L, L2\_FUND\_TRANSFER\_REPORT, amount);
32 uint64 sequence = wormhole.nextSequence(address(this));
33 wormhole.publishMessage(uint32(sequence), payload,
L, consistencyLevel);
34 }
35

Listing 2: L2WormholeRouter.sol (Line 40)

```
36 function requestFunds(uint256 amount) external {
37 require(msg.sender == address(vault), "Only vault");
38 bytes memory payload = abi.encode(Constants.L2_FUND_REQUEST,
44 amount);
39 uint64 sequence = wormhole.nextSequence(address(this));
40 wormhole.publishMessage(uint32(sequence), payload,
41 }
42
```

Listing 3: L1WormholeRouter.sol (Line 37)

```
29 function reportTVL(uint256 tvl, bool received) external {
30     require(msg.sender == address(vault), "Only vault");
31     bytes memory payload = abi.encode(Constants.L1_TVL, tvl,
4, received);
32     // NOTE: We use the current tx count (to wormhole) of this
4, contract
33     // as a nonce when publishing messages
34     // This casting is fine so long as we send less than 2 ** 32 -
4, 1 (~ 4 billion) messages
35     uint64 sequence = wormhole.nextSequence(address(this));
36
37     wormhole.publishMessage(uint32(sequence), payload,
4, consistencyLevel);
38 }
39
```

#### Listing 4: L1WormholeRouter.sol (Line 45)

```
40 function reportTransferredFund(uint256 amount) external {
41 require(msg.sender == address(vault), "Only vault");
42 bytes memory payload = abi.encode(Constants.
L_L1_FUND_TRANSFER_REPORT, amount);
43 uint64 sequence = wormhole.nextSequence(address(this));
44
45 wormhole.publishMessage(uint32(sequence), payload,
L, consistencyLevel);
46 }
47
```

#### Proof of Concept:

- 1. Wormhole publishMessage function increase its fee transaction
- 2. Affine DeFi wormhole routers fail to publish messages due to not sending any fee on the transaction
- 3. Affine DeFi overall protocol does not properly work

Risk Level:

Likelihood - 1 Impact - 5

### Recommendation:

Considering the need to call publishMessage, paying transaction fees is strongly recommended.

Remediation Plan:

**SOLVED**: The Affine DeFi team solved the issue in commit: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

### 3.2 (HAL-02) POSSIBLE LOSS OF FUNDS - MEDIUM

### Description:

Wormhole does not fail if the destination chain ID is different from the one supposed to be. If the rebalancer bot calls this function directly with a different chain ID, it will not fail, so funds during the transactions can be lost.

You can check the Wormhole Chain IDs on each chain, which is not the same as the network chain ID and can be easily confused.

Code Location:

```
Listing 5: WormholeRouter.sol (Line 43)
41 function _validateWormholeMessageEmitter(IWormhole.VM memory vm)
L, internal view {
42   require(vm.emitterAddress == bytes32(uint256(uint160(
L, otherLayerRouter))), "Wrong emitter address");
43   require(vm.emitterChainId == otherLayerChainId, "Wrong emitter
L, chain");
44   require(vm.nonce >= nextValidNonce, "Old transaction");
45 }
46
```

#### Proof of Concept:

- 1. Confuse wormhole chain ID with network chain ID
- 2. Initialize the contract with a wrong wormhole chain ID
- 3. Execute transactions on the protocol
- 4. Validate wormhole message emitter does not work as intended

Risk Level:

Likelihood - 1 Impact - 5

### Recommendation:

Creating a Chain ID whitelist with all the possible Chain IDs or having it hardcoded within the contract is recommended.

Remediation Plan:

**SOLVED**: The Affine DeFi team solved the issue in commit: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

### 3.3 (HAL-03) POSSIBLE UNPREDICTABILITY BETWEEN L2 AND L1 RATIOS - LOW

### Description:

When setLayerRatios function is used to update the ratio between L1 and L2, an invalid total ratio can be set (more than 100%). Hence, the rebalancer bot could not properly work in those cases.

Code Location:

```
Listing 6: L2Vault.sol (Lines 450,451)

449 function setLayerRatios(uint256 _l1Ratio, uint256 _l2Ratio)

L, external onlyGovernance {

450 l1Ratio = _l1Ratio;

451 l2Ratio = _l2Ratio;

452 }

453
```

Risk Level:

Likelihood - 2 Impact - 3

#### Recommendation:

When setting the ratios, making sure the total ratio is equal to 100% is recommended.

#### Remediation Plan:

RISK ACCEPTED: The Affine DeFi team accepted the risk of this finding.

### 3.4 (HAL-04) FUNCTION DOES NOT CHECK THE TOKEN BALANCE BEFORE AND AFTER A CALL - LOW

### Description:

Whenever the exit function is used, the contract should check the token balance before and after the call. So, the exact amount of tokens sent can be properly checked.

Code Location:

Listing 7: BridgeEscrow.sol (Line 64)

```
60 function l1ClearFund(uint256 amount, bytes calldata exitProof)
L, external {
61 require(msg.sender == wormholeRouter, "Only wormhole router");
62
63 // Exit tokens, after that the withdrawn tokens from L2 will
L, be reflected in L1 BridgeEscrow.
64 rootChainManager.exit(exitProof);
65
66 // Transfer exited tokens to L1 Vault.
67 uint256 balance = token.balanceOf(address(this));
68 require(balance >= amount, "Funds not received");
69
70 IL1Vault l1Vault = IL1Vault(vault);
71 token.safeTransfer(address(l1Vault), balance);
72
73 l1Vault.afterReceive();
74 }
75
```

Risk Level:

Likelihood - 2 Impact - 2

### Recommendation:

Checking the token balance before and after the exit call is recommended.

Remediation Plan:

**SOLVED**: The Affine DeFi team solved the issue in commit: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

## 3.5 (HAL-05) LACK OF PROPER SLIPPAGE PROTECTION - INFORMATIONAL }

### Description:

Within the <u>\_claimAndSellRewards</u> function, the slippage protection of the transaction is set to zero. Hence, if there is tiny liquidity, there is a high risk of losing part of the investment.

Code Location:

Lis	ting 8: L1CompoundStrategy.sol (Line 127)
122	<pre>function _claimAndSellRewards() internal {</pre>
	<pre>comptroller.claimComp(address(this));</pre>
124	if (rewardToken != address(cToken)) {
125	<pre>uint256 rewardTokenBalance = balanceOfRewardToken();</pre>
126	if (rewardTokenBalance >= minRewardToSell) {
	<pre>_sellRewardTokenForWant(rewardTokenBalance, 0);</pre>
128	}
129	}
	return;
131	}
132	

Risk Level:

Likelihood - 1 Impact - 1

Recommendation:

Setting at least 5% slippage protection is recommended.

Remediation Plan:

**SOLVED**: The Affine DeFi team solved the issue in commit: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

## 3.6 (HAL-06) POSSIBLE MISUSE OF CHAIN ID - INFORMATIONAL

### Description:

When initializing the wormhole router, the wormhole chain ID can be misused. As can be wrongly set due to confusion with the different deployed chain IDs.

As mentioned on HAL02, you can check the Wormhole Chain IDs on each chain, which is not the same as the network chain ID and can be easily confused.

### Code Location:

Listing 9:	L2WormholeRouter.sol	(Line	26)	
------------	----------------------	-------	-----	--

	nction initialize(IWormhole _wormhole, L2Vault _vault, address				
└→ _01	└→ _otherLayerRouter, uint16 _otherLayerChainId)				
	external				
20	initializer				
21 {					
22	wormhole = _wormhole;				
	<pre>vault = _vault;</pre>				
24	governance = vault.governance();				
25	otherLayerRouter = _otherLayerRouter;				
26					
27 }					
28					

### Risk Level:

Likelihood - 1 Impact - 1

### Recommendation:

As mentioned on HAL02, creating a Chain ID whitelist with all the possible Chain IDs or having it hardcoded within the contract is recommended.

Remediation Plan:

**SOLVED**: The Affine DeFi team solved the issue in commit: 06d6bc37fa80f0fdf794a8cb93e8100288d065e0

# AUTOMATED TESTING

### 4.1 STATIC ANALYSIS REPORT

#### Description:

Halborn used automated testing techniques to enhance the coverage of certain areas of the scoped contracts. Among the tools used was Slither, a Solidity static analysis framework. After Halborn verified all the contracts in the repository and was able to compile them correctly into their ABI and binary formats, Slither was run on the all-scoped contracts. This tool can statically verify mathematical relationships between Solidity variables to detect invalid or inconsistent usage of the contracts' APIs across the entire code-base.

### Slither results:

<text><code-block><code-block><code-block><code-block></code></code></code></code>

AUTOMATED TESTING

- amountWithdrawn = strategy.divest(tokenAmount) (contracts/BaseVault.sol#366) State variables written after the call(s): - strategies[strategy].balance - amountWithdrawn (contracts/BaseVault.sol#366)
- traisgare straight straight - annotation (contrais ann contrais ann
Reentrancy in BaseYault.depositIntoStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#323-339): External calls:
- strategy-inves(tokenAeount) (contracts/BaseYault.sol#337) Event emitted after the call(s): - StrategyDepositistrategy,tokenAeount) (contracts/BaseYault.sol#338)
Reentrancy in BaseVault.withdrawFromStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#342-376): External calls: - amountWithdrama = strategy.divest(tokenAmount) (contracts/BaseVault.sol#366)
<ul> <li>amountations/am = bitargs/idures(contention(), (contact/sates/area/contention))</li> <li>Fent emitted affer the call(s):</li> <li>- Strategy/ith/drawal(strategy,amountation#secult_sates/area/contention)</li> <li>Reference: https://gith/dc.mc/contention/erea/contenit/contention/erea/contention/erea/contention/contention/cont</li></ul>
BaseVault.harvest(BaseStrategy(]) (contracts/BaseVault.sol#407-462) uses timestamp for comparisons
Dangerous comparisons: - require(bool,string)(block.timestamp >= lastHarvest + lockInterval,PROFIT_UNLCOCTNG) (contracts/BaseVault.sol#409) BaseVault.lockd9rofit() (contracts/BaseVault.sol#468-475) uses timestamp for comparisons Dangerous comparisons:
- block.timestamp >= lastHarvest + lockInterval (contracts/BaseVault.so]#469) Reference: https://github.com/rytic/slither/wiki/Detector-Documentation#block-timestamp
<pre>Wulticall.multicall(bytes()) (contracts/external/Wulticall.sol49-27) uses assembly</pre>
BaseYault_remunsEtratagy/BaseStratagy/ (contact://BaseWult.sol240-771) has cottly operations incide a loop:
- totalBgs == stratinfo.tvlBgs (contracts/BaseVault.sol#240-271) has costly operations inside a loop: BaseVault.removeStrategy(BaseStrategy) (contracts/BaseVault.sol#240-271) has costly operations inside a loop: - totalStrategyHOIdings == loBal (contracts/BaseVault.sol#259)
Basfwlut.remov8frrstegy/BaseSfrrstegy/(contracts/Base/wult.scl240-72) has costly geprations inide a loop: - maliculedForfit += of dBal = magnuth/dfarm (contract/Base/wult.scl247)
BaseVault.updateStrategyAllocations(BaseStrategy(1),uint256(1)) (contracts/BaseVault.sol#278-297) has costly operations inside a loop: - totalBas = oldpa (contracts/BaseVault.sol#298) BaseVault.increaseVTURSp(uint256) (contracts/BaseVault.sol#286-218) has costly operations inside a loop:
- totalBps = newTotalBps (contracts/BaseVault.sol#200) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop
BaseYault_Liquidate(unr256) [contracts/BaseYault.sal#646-525) is newsr used and should be removed BaseYault.depositIntSitztegy(BaseSitz
Programmers version 08.8.13 (contracts/AfrineBowerneble.sol21) necesitates a version too recent to be trusted. Consider deploying with 0.4.6.70.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.170.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.170.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.170.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.170.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.170.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.1270.7.0/0.8.7 Programmers version 08.3.13 (contracts/BaskItangeworne) 04/201 necesitates a version too recent to be trusted. Consider deploying with 0.4.1270.7.0/0.8.7 Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) necesitates a version too recent to be trusted. Consider deploying with 0.4.1270.7.0/0.8.7 Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) necesitates a version too recent to be trusted. Consider deploying with 0.4.1270.7.0/0.8.7 Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) necesitates a version too recent to be trusted. Consider deploying with 0.4.1270.7.0/0.8.7 Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) Programmers version 08.3.13 (contracts/Interface/INDOCCMENDADAGEWORNE) Programmers version 08.3.13 (contr
Pragma version*0.8.13 (contracts/interfaces/compound/IComptroller.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 solc-0.8.16 is not recommended for deployment Reference: https://github.com/crytic/githe/riki/Detector-Documentation#incorrect-versions-of-solidity
lew level call in Multicall.Multicall(bytes()) (contracts/external/Multicall.sol#9-27): - (success.result) = addresulthidelegatesall(data[]) (contracts/external/Multicall.sol#12) Reference: https://github.com/prii/silthersult/acumentation#20=-2015
Variable BaseVault.smapWithdrawalQueueIndexes(uint256, uint256).newStrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.smapWithdrawalQueueIndexes(uint256, uint256, uint256).newStrategy2 (contracts/BaseVault.sol#131) is too similar to BaseVault.smapWithdrawalQueueIndexes(uint256, uint256, uint256
BridgeScrow.vullNonc (contracts/dridgeScrow.sol93) should be constant LidospoundStrategy.nindexerfdSell[contracts/dridgeScrow.sol93]) should be constant WarmbalRouter.nestVBlidNonce (contracts/WormbalRouter.sol935) should be constant WarmbalRouter.cotterLayerRouted (contracts/WormbalRouter.sol943) should be constant WarmbalRouter.cotterLayerRouted (contracts/WormbalRouter.sol943) should be constant WarmbalRouter.cotterLayerRouted (contracts/WormbalRouter.sol943) should be constant MarmbalRouter.cotterLayerRouted (contracts/WormbalRouter.sol943) should be constant
esset() should be declared external: - #setWalt.saset() (contracts/BaseYault.sol#83-36) basentialize(address,EDC2),address,EridgeEstrow) (contracts/BaseYault.sol#37-54) - BaseVault.baseThildsing(address,ERC2),address,EridgeEstrow) (contracts/BaseYault.sol#37-54)
vaulTVL() should be declared external: - Besevalt.vaulTVL() contracts/BaseVault.sol#478-480)
balanceOfTChekn() should be declared external: - LiCompoundStrategy.balanceOfTChekn() (contracts/ethereum/LiCompoundStrategy.sol#69-71) tetallockedValue() should be declared external:
<ul> <li>L1CompoundStrategy.totallockedValue() (contracts/ethereum/L1CompoundStrategy.sol#147-153) multicall(bytes()) should be declared external:         - Multicall.ustical(bytes()) (contracts/external/Multicall.sol#9-27)     </li> </ul>

### src/ethereum/L1Vault.sol

est = strategy.totalio:ke5Vslue() (contracts/BaseVsult.sol#432) ritten after the call(s): tegyibsince = balanceshidarvest (contracts/BaseVsult.sol#436) ofVL) (contracts/sthoreum/L1Vsult.sol#63-75): eRouter).reportTVL(tvl,received) (contracts/ethereum/L1Vault.sol#67) ter the call(s): cho call(5): /ethereum/L1Vault.sol#72) /slither/wiki/Detector-Docume mentation#reentrancv-vulnerabilities-1 (10)://dimensionary/id/simmension/id/contracts/SmeWault.sol4488) is a local variable never initialized rest(SmeStrategy(D).totalProfilectured (contracts/SmeWault.sol4219) is a local variable never initialized solance().neuntSolmeet( contracts/SmeWault.sol4265) is a local variable never initialized top://github.com/srtic/sil/bert/sik/Ovector/OvecmaintSolmentInitialized-cont-variables om/cfylic/sztums/Asso-sevent zracz/Basywult.sol850-500) ignores return value by strategy.divest(currStrategyTVL) – idealStrategyTVL) (contracts/BaseYault. uinz555,bool) contracts/sthereum/LWormholeRouter.sol820-38) ignores return value by mormhole.publishMessage(uint32(sequence) strateford/uist3f44 (contracts/sthereum/LWormholeRouter.sol840-66) ignores return value by mormhole.publishMessage(uint32(se consistencyLevel) (contracts/ethereum/L1WormholeRou avlaad.consistencyLevel) (contracts/ethereum/L1Worm }) uuter (contracts/ethereum/L1WormholeRouter.sol#18) lacks a zero-check on L1WormholeRouter.sol#25) ssing-zero-address-validation - otherLayerRouter = \_otherLayerRouter (contra : https://github.com/crytic/slither/wiki/Detector-Do noveffrategy(BaseStrategy) (contracts/BaseVault.sol#240-271) has external calls inside a loop: amountWithdram = strategy.divest(type()(uint256).max) (contracts/BaseVault.sol#257) vextBaseStrategy() (contracts/BaseVault.sol#240-271) has external calls inside a loop: balanceThisHarvest = strategy.divest(type()(uint256).max) (contracts/BaseVault.sol#257) valance() (contracts/BaseVault.sol#540-542) has external calls inside a loop: balanceThisHarvest = strategy.totalLockedValue() (contracts/BaseVault.sol#258) salance() (contracts/BaseVault.sol#540-542) has external calls inside a loop: sanountGinvest\_masst.balanceOf(saddrass(ult.sol#568) salance() (contracts/BaseVault.sol#540-549) has external calls inside a loop: tartegy.totalLockedValue() (contracts/BaseVault.sol#568) salance() (contracts/BaseVault.sol#540-549) has external calls inside a loop: tartegy.totalLockedValue() (contracts/BaseVault.sol#567) titarJ[tytes[]) (contracts/MassVault.sol#540-549) has external calls inside a loop: tartegy.totalLockedValue() (contracts/BaseVault.sol#567) titarJ[tytes[]) (contracts/external/MulticalLol#0-277) has external calls inside a loop: tartegy.totalLockedValue() (contracts/BaseVault.sol#567) titarJ[tytes[]) (contracts/external/MulticalLol#0-277) has external calls inside a loop: tartegy.totalLockedValue() (contracts/BaseVault.sol#567) External calis: - amountWithdrawn = strategy.divest(type()(uint286).max) (contracts/BaseYault.sol#257) State variables written after the calls(s): - malockepPorti = oldB1- amountWithdrawn (contracts/BaseYault.sol#267) - totalExtategyHoldings - oldB1 (contracts/BaseYault.sol#266) (on faseYault.withdrawFoordistegy LabsStategy uint256) (contracts/BaseYault.sol#362-376): ternal ealls: asountkithdram = strategy.divest(tokenAmount) (contracts/BaseVault.sol#B64) ate variables mritten after the call(B): strategististrategyhilane = amountkithdraam (contracts/BaseVault.sol#B66) totaldtrategyhilating = amountkithdraam (contracts/BaseVault.sol#B66) totaldtrategyhilating = amountkithdraam (contracts/BaseVault.sol#B66) totaldtrategyhilating = amountkithdraam (contracts/BaseVault.sol#B66) / in LiVault.\_transferFundsToL2(uint256) (contracts/ethereum/LiVault.sol#88-95): ternal calls: chainManage.depositere:.... tternl call: chaiMmager.AppoitFor(address(bridgeEscrow).address(\_sset).abi.encodePacked(amount)) (contracts/ethereum/LiVault.sol#90) LiNormbolROuter(wermholRouter).reportTamsforreffund(amount) (contracts/ethereum/LiVault.sol#93) wort maitted after the call[Li] fundTransforTol2[amount] (contracts/ethereum/LiVault.sol#94) j: m EmavYault.fepsilint/ofitatray(MaseFitatery\_unitS5) (contracts/BaseYault.sol#323-339): nr in Lanrmai wourd: treativerunds opras,pres) (contracts/stnerun/Linermai.enourd: solaru-ternan: colarus Event maited after the coll(s): - TransferFand(zamont) (contracts/stnerun/Linermai.enourd: Solarus my in Linu(zamont) (contracts/stnerun/Linermai.enourd: solaru) Event maited after the coll(s): - TransferFand(zamont) (contracts/stnerun/Linermai.enourd: solarus Event maited after the coll (s): Event maited after the coll (s): Evernal calls: - LiXorableAusUrfworableABouter).reportTVL(tv],reseived) (contracts/sthereum/LiXoult.sol#67) Event amitted after the call(s): - SendTVL(tv) (contracts/sthereum/LiXoult.sol#74) noy in BaseYault.withdrawFonStrategy(BaseStrategy,uin1266) (contracts/BaseYault.sol#362-376): External calls: - amountWithdrawm = strategy.divest(tokenAmount) (contracts/BaseYault.sol#364) Event amitted after the call(s): - StrategyWithdrawal(strategy,amountWithdrawm) (contracts/BaseYault.sol#374) = strategyWithdrawal(strategy,amountWithdrawm) (contracts/BaseYault.sol#374) = https://dimd.com/crytics/liter/swithdrawal(sol#374) ungergus comparisons: - require (boo),string(block.timestamp >= lastHarvast + lockInterval,PROFIT\_UNLOCKINO) (contracts/BaseYault.sol#460) BaseYault.lockedProfit() (contracts/BaseYault.sol#464-75) uses timestamp for comparisons Dengerous comparisons: - block.timestamp >= lastHarvast + lockInterval (contracts/BaseYault.sol#469) Reference: http://glinub.com/striid/slime/scli/Disterval-DomannitisonBlock-Limestamp Reference: http://glinub.com/striid/slime/scli/Disterval-DomannitisonBlock-Limestamp Reference: https://github.com/crytic/slither/wiki/Detector-Documentian#asemBj--usage BaseYult.resoveFirstegy(BaseTategy) (contracts/BaseYult.sol9540-471) has costly operations inside a loop: - totalBas -= strainfor.tvlBes (contracts/BaseYult.sol9540) - totalStrategy(bldings -= oldBal (contracts/BaseYult.sol9260) - totalStrategy(bldings -= oldBal (contracts/BaseYult.sol9260) - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - withDase - monorContent(BaseStrategy) (lostFastStateStudt) (contracts/BaseYult.sol9260) - withDase - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - withDase - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - withDase - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - withDase - maxicstedProfit == oldBal - amountWithdram (contracts/BaseYult.sol9260) - withDase - maxicstedProfit == oldBal - withDase - totalBase - totalBase - shopp - withDase - maxicstedBase(contracts/BaseYult.sol9260) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costlp-operations-inside-a-loop

Pragma version\*8.8.13 (contracts/AffineBovernable.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version\*0.8.13 (contracts/BaseSuitatey.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version\*0.8.13 (contracts/BaseSuitatey) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version\*0.8.13 (contracts/BaseSuitatey) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version\*0.8.13 (contracts/Bridgescrom.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version\*0.8.13 (contracts/Bridgescrom.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 int to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 cent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 int to recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 erent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.7.6/0.8.7 int 0.6.12/0.7.6/0.8.7 int 0.6.12/0.7.

ror deployment
:rytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

L1Vault (contracts/ethereum/L1Vault.sol#18-103) should inherit from IL1Vault (contracts/interfaces/IVault.sol#4-6) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-inheritance

iable BaseVault.swapWithdrawalQueuwIndexes(uint256,uint256).newGtrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.swapWithdrawalQu iable Constants.LI\_FUMD\_ITAMSFER\_REFORT (contracts/Constants.sol#22) is too similar to Constants.LI\_FUMD\_IMMSFER\_REFORT (contracts/Constants.sol#7) ernors: https://github.com/cryfic/slithtor/#situ/Betector-DecumentationAwrabibLemmes-are-too-similar

ategy (contracts/BaseStrategy.sol#9-48) does not implement functions: - BaseStrategy.balanceOfAsset() (contracts/BaseStrategy.sol#92)

BaseStrategy.divest(uint256) (contracts/BaseStrategy.sol# BaseStrategy.invest(uint256) (contracts/BaseStrategy.sol BaseStrategy.totallockedValue() (contracts/BaseStrategy.s : https://github.com/crytic/slither/wiki/Detector-Document

BridgeEscrew.vaultNonce.(contracts/AzidgeEscrew.solat9) should be constant Reference: https://github.com/crytic/slither/wiki/Detestor-Documentation#state-variables-that-could-be-declarad-constant

writeme: https://giuno.tow/splis/splite

### src/ethereum/L1WormholeRouter.sol

- tation#dangerous-strict-equalities

- calls: ThisNervet = strategy.totllockedValue() (contracts/BaseVault.sol#432) imbles written after the call(s): ins(strategy).maines = maineorThisNervest (contracts/BaseVault.sol#435) Mult.sol#435) (contracts/ethersum/LIVault.sol#63-75):
- rmal calls: MormholaRouter(wormholaRouter).reportTVL(tyl,received) (contracts/sthereum/L1Vault.sol#67) e variables written after the call(s): coived = false (contracts/sthereum/L1Vault.sol#72) ttps://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulmerabilities-1
- wult\_organizeWithdrawelQouwe().offset (contract/Sere/wult.sol#220) is a local variable never initialized wult.maxwet(SereSizetey()).totalProfiderund (contract/Sere/Wult.sol#43) is a local variable never initialized wult.reholmoch).somontFolmers(contract/Sere/Wull:sol#54) is a local variable never initialized ence: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-local-variables

lance() (contracts/8aseVault.sol8540-590) ignores return value by strategy-divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol ter.reportTVL(uin1256,bool) (contracts/ethereum/LiMormholeRouter.sol820-38) ignores return value by wormhole.publishMessage(uin132(sequence),pas er.reportTransforzedFund(uin1256) (contracts/ethereum/LiMormholeRouter.sol840-46) ignores return value by wormhole.publishMessage(uin132(sequence),pas gs//github.corytic/silthereum/cimc266) comunentiantHumusdeTexturn , d,consistencyLevel) (contracts/ethereum/L1WormholeRout ,payload.consistencyLevel) (contracts/ethereum/L1Wormh

- http://gliub.com/crystrc/situar/sucrystrc/situar/sucrystructures removisitarg/safstrcay() contracts/Safstylut.csl260-27) has external calls insids a log: securitWithdram = strategy.divest(type()(uint26).max) (contracts/Safstylut.csl2637) harvest(Basstrategy()) contracts/Safstylut.csl2640-7402) has external calls insids a log: blanceflinderwat = strategy.totalcckedfulu() contracts/Safstylut.csl26437) reblance() contracts/Safstylut.csl2640-7402) has external calls insids a log: strategy.texp.tslateckedfulu() contracts/Safstylut.csl26437) reblance() contracts/Safstylut.csl2640-7500) has external calls insids a log: strategy.tslateckedfulu() contracts/Safstylut.csl26387) reblance() contracts/Safstylut.csl2640-5500) has external calls insids a log: currategy.tsequettGrvetty/t = strategy.totalccedfulu() contracts/Safstylut.csl26387 reblance() contracts/Safstylut.csl2640-5500) has external calls insids a log: currategy.tsequettGrvetty/t = strategy.tsl2000 reblance() contracts/Safstylut.csl2640-5500) has external calls insids a log: strategy.tsl2000 for the strategy.tsl2000 for the

- - rence: https://github.cow/cryic/dithuf/wiki/detector-Decumentation/wealls-inside=a-loop
    trancy in BaseVault.resoved(saseStrategy) (contracts/BaseVault.sol#240-271):
    External calls:
     - assountWindsam = strategy.divest(type()(uint250.max) (contracts/BaseVault.sol#257)
    State variables writen after the call(s):
     - maxicode/orfit ts.cldBat = assountWindsam (contracts/BaseVault.sol#267)
    trancy in BaseVault.sol#260-278):
    External calls:
     - assountWindsam codStrategy.divesStrategy.uin260) (contracts/BaseVault.sol#262-378):
    External calls:
     - assountWindsam restrategy.dives(tokenAssount) (contracts/BaseVault.sol#262)
     - strategiselse writen after the call(s):
     - strategiselse writen after the call(s

Reentrancy in L1Vault_transferFundsToL2(uint256) (contracts/ethereun/L1Vault.sol#88-95): Enternal calls: haimManger.depositFor(address(bridgeEscrow),address(_asset),abi.encodePacked(amount)) (contracts/ethereum/L1Vault.sol#98)
- L1WormholeRouter(wormholeRouter).reportTransferredFund(amount) (contracts/ethereum/L1Vault.sol#93) Event emitted after the call(s):
<ul> <li>FundTransferToL2(amount) (contracts/ethereum/L1WaUt.sol994)</li> <li>Rentrancy in BaseVaUt.depositIntOstracterg(BaseStracterg, uint256) (contracts/BaseVaUt.sol8323-339):</li> </ul>
External calls: - stratagy.invest(tokenAmount) (contracts/BaseYault.sol#337)
Event emitted after the call(s): - StatesynOppositaterstap,tokenMegunt) (contracts/BaseYault.sol#388)
Reentrancy in 11Yault.processFundBequest(uint266) (contracts/ethereum/L1Yault.sol#78-83): External calls: — _ liquidate(amountRequested) (contracts/ethereum/L1Yault.sol#80)
l1qub&FelamontHedgeste0 (contracts/stefferum/LivalL:SolBe0) - amontHetMerma = stategs_divestiteAmenumU (contracts/BaseVault.sol#364) transferfundStoL2(amountDSomd) (contracts/stheraum/LIVault.sol#32) chaimAmenger- dopsitforsidafenss birdgeStcores,address(_asset),abi.encodePacked(amount)) (contracts/sthereum/LIVault.sol#98)
later to be a set of the set
- L1WormholeRouter(wormholeRouter).reportTransferredFund(amount) (contracts/etheraum/L1Vault.sol#93) Event emitted after the call(s): - FundTransferTulZaumut) (contracts/etheraum/L1Vault.sol#94)
<ul> <li>_ transferfundsTol2(amountToSend) (contracts/sthereum/L1%ult.sol882)</li> <li>Rentrancy in Liborahol@houter.receivefunds(bytes, bytes) (contracts/sthereum/L1%unten)al@houter.sol850-62):</li> </ul>
External calls: - vault.bidgeEsrow().llClearFund(amount,data) (contracts/ethereum/LlWormholeRouter.sol#60)
Event emitted after the call(s): - TransferFromL2(mmount) (contracts/thereum/LiMormholeRouter.sol#61) Reentrancy in LiVault.sondTVL() (contracts/ethereum/LiMoult.sol#63-75):
External calls:
- LNGrehol#Gouter(worshol#Gouter).reportTVL(tvl,received) (contracts/ethereum/LN9ult.sol#67) Event emitted after the call(s): - SamTV(tvl) (contracts/ethereum/LN9ult.sol#74)
Reentrancy in BaseVault.withdrawFromStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#362-376):
External calls: - meanufilthiran = stategy.divest(tokenAmount) (contracts/BaseVault.sol#366)
Event emitted after the call(s): - StrategyWithdrawal(strategy,mountWithdrawn) (contracts/BaseVault.sol#374) Reference: https://githbu.com/syrlio/slither/wiki/Detector-Documentation#renntrancy-vulnerabilities-3
ne srame . nrupryglindorum /
Dangerous comparisons:
— require(bool,string)(block.timestamp >= lastHarvest + lockInterval,PROFIT_UNLOCKING) (contracts/BaseVault.sol#409) BaseVault.lockedProfit() (contracts/BaseVault.sol#468-475) uses timestamp for comparisons Dangerous comparisons:
<ul> <li>- Diock.timestmap &gt;= lastNarvast + lockInterval (contracts/NasvAvult.sa)14640)</li> <li>Reference: http://github.com/controls/NatvAvult.sa)14640)</li> </ul>
<pre>Multicall(bytes()) (contracts/external/Multicall.sol#9-27) uses assembly</pre>
- TNLINE ASM (contracts/sterna)/Multicall.sol357-21) Perference: http://gliubi.com/stivi/Detector-Documentation#assembly-usage
BaseYault.removeStrategy(BaseStrategy) (contracts/BaseVault.scl#248-272) has costly operations inside a loop:
<ul> <li>totalBps == stratinfo.tvlBps (contracts/BaseWault.sol#248-271) has costly operations inside a loop:</li> <li>totalStrategy(BaseStrategy) (contracts/BaseWault.sol#248-271) has costly operations inside a loop:</li> <li>totalStrategy(BaseBurg) == oldBal (contracts/BaseWault.sol#258)</li> </ul>
<ul> <li>- totalStrategWoidings -= cldBal (contracts/BaseValLs.02F257)</li> <li>Barkult.remov/StrategWienstrategW</li></ul>
Saravan under Stringen location (Marstrand International Contest/Saravan) (Saravan) (S
<ul> <li>totalBps -= oldBps (contracts/BaseYault.sol#293)</li> <li>BaseYaut.increaseTtLBps/uint250 (contracts/BaseYault.sol#286-218) has costly operations inside a loop:</li> <li>totalBps ==meTotalBps (contracts/BaseYault.sol#280)</li> </ul>
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation≇costly-operations-inside-a-loop
LLYaultmsgData() (contracts/ethereum/LLYault.sol#50=52) is never used and should be removed Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
Pragma version%.8.13 (contracts/Affindevernable.sol22) necessitates a version too recent to be trusted. Consider deploying with 0.4.12(0.7.4/0.8.7 Pragma version%.8.13 (contracts/BaseStrategy.ol22) necessitates a version too recent to be trusted. Consider deploying with 0.4.12(0.7.4/0.8.7 Pragma version%.8.13 (contracts/BaseStrategy.ol22) necessitates a version too recent to be trusted. Consider deploying with 0.4.22(0.7.4/0.8.7 Pragma version%.8.13 (contracts/BaseStrategy.ol22) necessitates a version too recent to be trusted. Consider deploying with 0.4.22(0.7.4/0.8.7 Pragma version%.8.13 (contracts/Hindpeisrem.ol22) necessitates a version too recent to be trusted. Consider deploying with 0.6.22(0.7.4/0.8.7)
Prana version 0.8.31 (contracts/horhouts.size) necesities version too include too be traited sporting in bizards/sporting 6.7 Prana version 0.8.33 (contracts/horhouts/size) necesities version too recent to be traited. Consider sporting 8.17(7,1,6,6,6,7)
<pre>right Verlief 0.13 (contract/distruction)// destitutes a version to feamt to be truited. Consider deploying with 0.4.21/0.7.0/0.4.7</pre>
Pragma version®.8.13 (contracts/interfaces/IVault.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version®.8.13 (contracts/interfaces/Normhole.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 sol=0.8.16 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
low level call in Multicall.multicall.dytes()) (contrats/sternal/Multicall.sol09-27): - (success.scult = adversethii / depreselidetical) (contrats/sternal/Multicall.sol012) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
LlVault (contracts/ethereum/LlVault.sol#18-183) should inherit from ILlVault (contracts/interfaces/IVault.sol#4-6) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-inheritance
Variable SassVault.saspMithdramalDowatndowas(uint256).nemStratogy1 (contracts/SassVault.sublit) is too sisilar to BassVault.saspMithdramalDowauIndowas(uint256,uint256).nemStratogy2 (contracts/ Variable Constants.li,EUMD_TRAMSER_REPORT (contracts/Constants.gol#12) is too similar to Constants.l2,FUND_TRAMSER_REPORT (contracts/Constants.sol#7) Reference: https://github.com/cytic/siltmar/ski/DMtette-DocumentationMariable-mass=are-too-similar
BasStrategy (contracts/BasStrategy.sol#9-48) does not implement functions: - BassStrategy.solanceOfAsset() (contracts/BasStrategy.sol225) - BasStrategy.divet(unit28) (contracts/BasStrategy.sol246)
- BaseStratey, invest(uin1256) (contractv(BaseStratey).sol238) - BaseStratey, totalLockeVilue() (contractv(JaseStratey).sol24) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unimplemented-functions
BridgeEscrow.vallNonce (contracts/BridgeEscrow.solP19) should be constant Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
asset() should be declarad external: - BaseVaul.asst() (contasts/BaseVault.sol#33-35) - initialize/address.Bridgedtecrom,RootChainWanager,address) should be declared external:
<ul> <li>LIYault.initialize(address,ERC20,address,BridgeEscrow,IROotChsinManager,address) (contracts/sthereum/LIYault.sol#31-44)</li> <li>Multiallbytes(1) should be declared external:</li> <li>Multial.nuticall(hytes(1)) (contracts/external/Multicall.sol#9-27)</li> </ul>

### src/external/Multicall.sol

Multicall.multicall(bytes[]) (contracts/external/Multicall.sol#9-27) has external calls inside a loop: (success,result) = address(this).delegatecall(data[i] Reference: https://github.com/crytic/slither/wiki/Detector-Documentation/#calls-inside-a-loop	
Mulicall.mulicall(bytes[]) (contracts/ssternal/Mulicall.sol#9-27) uses assembly - InLME ASM (contracts/ssternal/Mulicall.sol#9-21) Reference: Https://githul.comt/grits/lithts/ski/lotecto-Documentation#assembly-usage	
Pragma version*0.8.13 (contracts/external/Multicall.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 solt=0.8.16 is not recommended for deployment Reference: https://github.com/cyritic/alither/kiki/Detector-Documentation#incorrect-versions-of-solidity	
low level call in Multicall.Multicall(bytes()) (contracts/external/Multicall.sol#0-270; - [succes,result] = address(thi).delegatecall(stat(j)) (contracts/external/Multical.sol#12) Reference: https://gitubu.com/gri/solither/sult/dotects-documentational0-avel-calls	
<pre>multicall(bytes[]) should be declared external: - Multicall.multicall(bytes[)) (contracts/external/Multicall.sol#9-27) Reference: Merch (with the contracts/external/Multicall.sol#9-27)</pre>	

src/polygon/Detailed.sol Prayma version\*0.8.13 (contracts/polygon/Detailed.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Reference: https://github.com/crytic/pitter/wiki/Detactor-Documentation#incorrect-versions-of-solidity

### src/polygon/EmergencyWithdrawalQueue.sol

	Multicall.multicall(bytes[]) (contracts/external/Multica	IL sol#9-27) has delegatecall inside a loop in a payable function: (success,result) = address(this).delegatecall(data[i]) (contracts/external/Multicall.sol#12
		or-Documentation/#payable-functions-using-delegatecall-inside-a-loop
	sasestrategy.vauit (contracts/Basestrategy.soi#13) is ne - BaseStrategy.sweep(ERC20) (contracts/BaseStrat BaseStrategy.asset (contracts/BaseStrategy.sol#21) is ne	ver initialized. it is used in: egy.sol#43-47) ver initialized. It is used in:
	<ul> <li>BaseStrategy.sweep(ERC20) (contracts/BaseStrat Reference: https://github.com/crytic/slither/wiki/Detect</li> </ul>	egy.sol#43-47) or-Documentation#uninitialized-state-variables
	L2VaultassessFees() (contracts/polygon/L2Vault.sol#62- -feesBps = (duration * managementFee) / SECS_PER	73) performs a multiplication on the result of a division: _YEAR (contracts/polygon/L2Vault.sol#66)
	-numSharesToMint = (feesBps * totalSupply()) / M Reference: https://github.com/crytic/slither/wiki/Detect	AX_BPS (contracts/polygon/L2Yault.sol#67) or-Documentation#divide-before-multiply
	L2VaultassessFees() (contracts/polygon/L2Vault.sol#62- - numSharesToMint == θ (contracts/polygon/L2Vaul	73) uses a dangerous strict equality: t.sol#69)
	L2VaultconvertToAssets(uint256,L2Vault.Rounding) (cont - totalShares == θ (contracts/polygon/L2Vault.so 12Vault.convertToShares(uint256,L2Vault Rounding) (cont	racts/polygon/l2Vault.sol#361-373) uses a dangerous strict equality: 1#363) racts/nolynon//2Vault.sol#360-363) uses a dangerous strict equality:
	- totalShares == 0 (contracts/polygon/L2Vault.so BaseVault.rebalance() (contracts/BaseVault.sol#549-590)	18364) uses a dangerous strict equality:
	<ul> <li>- amountToInvest == 0 (contracts/BaseVault.sol#b</li> <li>L2Vault.receiveTVL(uint256,bool) (contracts/polygon/L2Va</li> <li>- delta == 0 (contracts/polygon/L2Vault.sol#502)</li> </ul>	84) ult.sol#477-506) uses a dangerous strict equality:
	External calls: - redeemedåssetämpunt - vault redeemByEmergencyM	the second states and the second states with the second states and the second states and the second states and the second states and se
	State variables written after the call(s): - headPtr += 1 (contracts/polygon/EmergencyWithd Reentrancy in BaseVault.harvest(BaseStrategv[1) (contrac	rawalQueue.so1#93) fs/RaseAult.so1#407-462):
	State variables written after the call(s): - strategies[strategy].balance = balanceThisHarv Reference: https://uithub.com/crvtic/slither/wiki/Detect	est (contracts/BaseVault.sol#435) or-Documentationfreentrancy-vulnerabilities-1
	L2VaultcomputeRebalance().invest (contracts/polygon/L2 BaseVault.harvest(BaseStrategy[]).totalProfitAccrued (co BaseVaultorganizeWithdramalQueue().offset (contracts/8	Vault.SolPDb) 13 a local variable mever initialized ntracts/BaseVault.solP418) is a local variable mever initialized aseVault.solP229) is a local variable mever initialized
	Reference: https://github.com/crytic/siither/wiki/betect	or-bocumentationwuninitialized-local-variables
	L2WormholeRouter.requestFunds(uint256) (contracts/basevault.sols649-598) L2WormholeRouter.requestFunds(uint256) (contracts/polygo	agnese recent ware of setting, oriented interreprise - leaderstagerie ( consistency) and setting, oriented inter Lipolyon/LW-mohaReuter.sol#38-41) (ontracts/polyon/LZWormhole.publishMessage(uint32[sequence],payload,consistencyLevel) (contracts/polygon/LZWormholeReuter.s n/LZWormholeReuter.sol#38-41) ignores return value by wormhole.publishMessage(uint32[sequence],payload,consistencyLevel) (contracts/polygon/LZWormholeReuter.s
<pre>n - normal - grounds - grounds - grounds - location - DID</pre>	BaseVault.baseInitialize(address,ERC20,address,BridgeEsc	row) (contracts/BaseVault.sol#37-54) should emit an event for:
	- governance = _governance (contracts/BaseVault.	so1#42)
<pre>Number of the state of the</pre>	L2Vault.setManagementFee(uint256) (contracts/polygon/L2V - managementFee = feeBps (contracts/polygon/L2Va	ault.sol#54-56) should emit an event for: ult.sol#55)
<pre>very time = relative = relat</pre>	L2Vault.setWithdrawalFee(uint256) (contracts/polygon/L2V - withdrawalFee = feeBps (contracts/polygon/L2Va	ault.sol#58-60) should emit an event for: ult.sol#59) 
<pre>very time = relative = relat</pre>	L2vault.initialize(address, Exc20, address, bridgescrow, en - l1Ratio = _l1Ratio (contracts/polygon/L2Vault. - l2Ratio = _l2Ratio (contracts/polygon/L2Vault.	ergencymithdrawaluueue,audress,uintzbo,uintzbo,uintzbol/j/ (contracts/polygon/lzvault.sol#85-il#/ should emit an event for: sol#1800 sol#1810
<pre>Null result([unit()]; [unit()]; [unit()];</pre>	<ul> <li>withdrawalFee = fees[0] (contracts/polygon/L2V - managemenFee = fees[1] (contracts/polygon/L2V L2Vault setLaverBatics(uint256) (contracts/polygon/L2V     </li> </ul>	ault.sol#188) ault.sol#1899 pon(12%ult.sol#409-459) should amit an avent for:
<pre>r - relationship / relationship</pre>	<ul> <li>- 11Ratio = _11Ratio (contracts/polygon/L2Vault.</li> <li>- 12Ratio = _12Ratio (contracts/polygon/L2Vault.</li> </ul>	vii/ccaravii/oc/ siculd emit an event (c). sol#459)
<pre>frame. frame. fram</pre>	L2Vault.receiveTVL(uint256,bool) (contracts/polygon/L2Va - maxLockedTVL = lockedTVL() + totalProfit (cont - L1TotallockedValue = tvl (contracts/polygon/L2	ult.sol#477-506) should emit an event for: racts/polygon/L2Vault.sol#497) Vault.sol#499
<pre>i - ower _ sect _ intro termination function of the intro termination of the intro terminat</pre>	Reference: https://github.com/crytic/slither/wiki/Detect	or-Documentation#missing-events-arithmetic
<pre>intro = hemological = hem</pre>	– owner = owner (contracts/BridgeEscrow	- so1#29)
<pre>starsh:harhitistiqteders.UCS, address.UCS, address.tell</pre>		
<pre></pre>	- governance = _governance (contracts/Ba BaseVault.baseInitialize(address,ERC20,address,BridgeEsc	rew)wormholeRouter (contracts/BaseVault.sol#37) lacks a zero-check on :
<pre>representations.feed.accuberted(sci2b) (contract(/sci2berted(sci2b)) (contract(/sci2berted(sci</pre>	<ul> <li>wormholeRouter = _wormholeRouter (cont L2WormholeRouter.initialize(IWormhole,L2Vault,address,ui - otherLayerRouter = _otherLayerRouter (</li> </ul>	racts/BaseVauit.solf444) nt16)otherLayerRouter (contracts/polygon/L2WormholeRouter.sol#18) lacks a zero-check on : contracts/polygon/L2WormholeRouter.sol#25)
<pre>statu: Interest(BestStatus)    [contract/parameter(.sc)#status) = status [so]: status = status) = tatus =</pre>		
<pre>statu: Interest(BestStatus)    [contract/parameter(.sc)#status) = status [so]: status = status) = tatus =</pre>	<pre>comper() (contracts/polygon/EmergencyWithdrawalQueue.sol# BaseVault.removeStrategy(BaseStrategy) (contracts/BaseVa</pre>	<pre>xypoignncmergencymicnorawaluguessiev/-iz0 nas external calls inside a loop: redeemenasseramount = vauit.redeemegreergencymicnorawalugueucptr,witnorawalug d46-1080 ult.sol#240-271) has external calls inside a loop: amountWithdrawn = strategy.divest(type()(uint256).max) (contracts/BaseVault.sol#257)</pre>
<pre>status intering in the intering is a logic entropy of the intering is a logic entropy of the intering of the intering is a logic entropy of the interin</pre>	BaseVault.harvest(BaseStrategy[]) (contracts/BaseVault.s BaseVault.rebalance() (contracts/BaseVault.sol#549-590) BaseVault.rebalance() (contracts/BaseVault.sol#562-590)	ol#407-662) has external calls inside a loop: balanceThisHarvest = strategy.totalLockedValue() (contracts/BaseVault.sol#432) has external calls inside a loop: amountFolrvest = Math.min(amountFolrvest_asset.balanceOf(address(this))) (contracts/BaseVault.sol#583) has external calls inside a loop: stratewy recons 1 invest@amountFolrvest(contract#BaseVault.sol#581)
<pre>rtanks: http://gitub.com/cpic/situb/s</pre>	BaseVault.rebalance() (contracts/BaseVault.sol#549-590) BaseVault.rebalance() (contracts/BaseVault.sol#549-598)	nas externa ceras insure a loop, strategy_ecoup_interest (normest) (normest) (normest) (normest/strategyadoo) has external calls inside a loop: surstrategy.tetailceked(value() (contracts/BaseVault.sol#565) has external calls inside a loop: strategy.divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol#567)
<pre>kternal calls: liquétaissouril contract/phygon/LYNult.sel#St tran for liquétaissouril contract/phygon/LYNult.sel#St - tran for liquétaissouril contract/phygon/LYNult.sel#St tran for liquétaissouril contract/phygon/LYNult.sel#St Stat Variables article after the calls tran for liquétaissouril contract/phygon/LYNult.sel#St Stat Variables article after the calls tran for liquétaissouril (contract/phygon/LYNult.sel#St) tran for liquétaissouril (contract/phygon/LYNult.sel#St) tra</pre>	Multicall.multicall(bytes[]) (contracts/external/Multica Reference: https://github.com/crytic/slither/wiki/Detect	ll.sol#=-27) has external calls inside a loop: (success,result) = address(this).delegatecali(dats[i]) (contracts/external/Multicall.sol#12) or-Documentation/#calls-inside-a-loop
<pre>- securitidriams = trategy.divst(tokenkeout) (contract/sekvult.sel283) - transfertilssmithesing incomparised in the interverse interverse</pre>	External calls:	
<pre>- LNormbol@outr(cornbol@outr(.reportransforedFund(securt)(centratt/polygen/LYault.sol#552) staty wrights article wright to melling prof/Yault.sol#553) centransfortil = fols (centratt/polygen/LYault.sol#555-561); Extrumi_cols: centransfortil = fols (centratts/polygen/LYault.sol#555-561); Extrumi_cols: centransfortil = fols (centratts/polygen/LYault.sol#556) centransfortil = fols (centratts/polygen/LYault.sol#556); Extrumi_cols: centransfortil = fols (centratts/polygen/LYault.sol#556); Extrumi_cols: centransfortil = fols (centratts/polygen/LYault.sol#550); Extrumi_cols: centransfortil = fols (centratts/polygen/LYault.sol#550); Extrumi_cols: centransfortil = fols (centratts/polygen/LYault.sol#540); centransfortil = fols (centratts/polygen/LYault.sol#540);</pre>	- amountWithdrawn = strategy.divest(toke	nAmount) (contracts/BaseVault.sol#364)
<pre>- configneration: = fails (contracts/polygon/Zywult.self460) - configneration: contracts/polygon/Zywult.self457-5601; - configneration: = fails (contracts/polygon/Zywult.self457-5601; - configneration: = fails (contracts/polygon/Zywult.self457-5601; - configneration: = fails (contracts/polygon/Zywult.self450) - configneration: = stratego.divection: = fails (contracts/polygon/Zywult.self450) - configneration: = stratego.divection: = fails (contracts/polygon/Zywult.self450) - configneration: = fails (contracts/polygon/Zywult.self450) - configneration: = stratego.divection: = fails (contracts/polygon/Zywult.self450) - configneration: = stratego.divection: = fails (contracts/polygon/Zywult.self450) - configneration: = stratego.divection: = fails (contracts/polygon/Zywult.self450) - configneration: = stratego.divec</pre>	<ul> <li>L2WormholeRouter(wormholeRouter), report</li> </ul>	tTransferredFund(amount) (contracts/polygon/L2Vault.sol#552)
<pre>entrary in L2Vaildivertramillowith (contract/polyon/L2Vail.sol#557-561):</pre>	- canTransferToL1 = false (contracts/pol	ygon/L2Vault.sol#548)
<pre>State writeBise write state (contract/splygen/lYuli:sl#55) - contexputitemati = file - contexputitemati = file - contexputitemati = file - contexputitematic = file - contexputite</pre>	Reentrancy in L2VaultdivestFromL1(uint256) (contracts/ External calls:	polygon/LZVault.sol#557-561): amount) (contracts/oolyoon/L2Vault.sol#558)
<pre>External calls:</pre>	State variables written after the call(s): - canRequestFromL1 = false (contracts/polygon/L2	
<pre>State variables writes after the coll(s):</pre>	External calls: - bridgeEscrow.12Withdraw(amount) (contracts/pol	
<pre>entrany in BaseVault.ramyvättagy (sostratty) (contract/BaseVault.solf26-77):</pre>	State variables written after the call(s):	
<pre>State variables writes after the call(s): - main control i - mean contract / MassWall.sol #267) - main control i - mean contract / MassWall.sol #267) entrempy in MarkYwil.selfserredwrites / MassWall.sol #262-376): External calls: - manuntWithdram = strategy.divestickenAssumt) (contract / MassWall.sol #362-376): External calls: - manuntWithdram = strategy.divestickenAssumt) (contract / MassWall.sol #362-376): External calls: - manuntWithdram = strategy.divestickenAssumt) (contract / MassWall.sol #362-376): - total StrategyIndUstop: = monuntWithdram (contract / MassWall.sol #262) - total StrategyIndUstop: = monuntWithdram (contract / MassWall.sol #264) - transferTotil (MassUnt (contract / Contract / MassWall.sol #264) - transferTotil (MassUnt (contract / Contract / MassWall.sol #264) - transferTotil (MassUnt (contract / MassWall.sol #264) - transferTotil (MassUnt (contract / MassWall.sol #364) - transferTotil (MassUnt (contract / MassWall.sol #363) - transferTotil (MassUnt (Contract / MassWall.sol #364) - transferTotil (MassUnt (Contract / MassWall.sol #365) Exercised # fort the call(s): - TransferTotil (MassUnt (Contract / MassWall.sol #365) - transferTotil (MassUnt (Contract / MassWall.sol #365) - transferTotil (MassUnt (Contract / MassWall.sol #365) - transferTotil (MassWall</pre>	Reentrancy in BaseVault.removeStrategy(BaseStrategy) (co External calls:	ntracts/BaseVault.sol#240-271):
<pre>- totalStrategyholding = oldBal (contracts/BaseYault.soldESD) - totalStrategyholding = slategy.divertiteWalt.soldESD (contracts/BaseYault.soldESD) - totalStrategyholding = soundEvolute = soundEvol</pre>	State variables written after the call(s): - maxLockedProfit += oldBal - amountWithdrawn (c	ontracts/BaseVault.sol#267)
<pre>- asuutkithdram = strategy.divest(tekenkeunt) (contrate/BaseVault.sol#36) State variations = strategy.divest(tekenkeunt) (contrate/BaseVault.sol#36) State variations = manutkithdram (sou#Astrate) - strategiestErrategi.haines - manutkithdram (sou#Astrate) - strategiestErrategiest</pre>	<ul> <li>totalStrategyHoldings -= oldBal (contracts/Bas Reentrancy in BaseVault.withdrawFromStrategy(BaseStrateg</li> </ul>	eVault.sol#259)
<pre>- totalStategyHolding -= amountWithdramn (contract/BaseYault.sol#371) ference: http:://dithub.com/cry/id/inthuf/cam/cry/id/id/id/id/id/id/id/id/id/id/id/id/id/</pre>	- amountWithdrawn = strategy.divest(tokenAmount)	
<pre>entrang: in L2Vailtill2Beblance(boo).uint256) (contracts/polygon/L2Vailt.sol#527-538): External calls: liquidate(amount) (contracts/polygon/L2Vailt.sol#531) - assountWithdram = strategy.eivst(tokenAmount) (contracts/BaseVault.sol#564) - transferToil[smountContracts/polygon/L2Vailt.sol#543] - bajdetsree.invitidate(amount) (contracts/polygon/L2Vailt.sol#562) Event emitted after the call(s): - transferToil[smountContracts/polygon/L2Vailt.sol#563] - transferToil[smountContracts/polygon/L2Vailt.sol#563] event emitted after the call(s): - transferToil[smountContracts/polygon/L2Vailt.sol#553]); entrang: intL2VailtdivertToil(intext).contracts/polygon/L2Vailt.sol#553); entrang: intL2VailtdivertTointContracts/polygon/L2Vailt.sol#557-551);</pre>	<ul> <li>strategies[strategy].balance -= amountWithdraw</li> <li>totalStrategyHoldings -= amountWithdrawn (cont</li> <li>Reference: https://oithub.com/crutic/slither/wibi/Datast</li> </ul>	n (contracts/BaseVault.sol#366) racts/BaseVault.sol#371) or Documentation/sentracev-wilnerabilities-2
<ul> <li>_liquidate(amount) (contracts/polygon/LYuuit.sol#S31)</li> <li>_ amounti(indisame = strategg.sites(tokenAmount) (contracts/BaseVault.sol#S64))</li> <li>_ transferToil(amount/Sand) (contracts/polygon/LYuuit.sol#S64))</li> <li>_ brightsrame, liviindrame(amount) (contracts/polygon/LYuuit.sol#S65))</li> <li>Event emitted after the call(s):</li> <li>_ transferToil(amount) (contracts/polygon/LYuuit.sol#S64))</li> <li>_ transferToil(amount) (contracts/polygon/LYuuit.sol#S63))</li> <li>_ transferToil(amount) (contracts/polygon/LYuuit.sol#S63));</li> <li>_ transferToil(amount) (contracts/polygon/LYuuit.sol#S63));</li> <li>entransferToil(amount) (contracts/polygon/LYuuit.sol#S63));</li> </ul>	Reentrancy in L2VaultL1L2Rebalance(bool,uint256) (cont	
<pre>transferToLi(securitosind) (contractiv/polygon/L2Vault.solB53)</pre>	liquidate(amount) (contracts/polygon/L2Vault. - amountWithdrawn = strategy.divest(toke	nAmount) (contracts/BaseVault.sol#364)
Event emitted after the call(s): - Transferfoliameunt (contract/s)ugon/LZVault.sol#634) - Transferfoliameunt (contract/solypon/LZVault.sol#633) entrany in LZVault, divestfrantiduction (contracts/solypon/LZVault.sol#637-561): 	<ul> <li>transferToL1(amountToSend) (contracts/polygon</li> <li>_ bridgeEscrow.12Withdraw(amount) (contr</li> </ul>	/L2Yault.sol#533) acts/polygon/L2Yault.sol#543)
rranferToll(mountOstend) [contract/polygon/lYault.sol#53) entrany [LYault,_divertTontIuluit58] (contract/polygon/lYault.sol#53)	Event emitted after the call(s): - TransferToL1(amount) (contracts/polygon/L2Vaul	
<pre></pre>	<ul> <li>transferToL1(amountToSend) (contracts Reentrancy in L2VaultdivestFromL1(uint256) (contracts/</li> </ul>	/polygon/L2Vault.sol#533)
	<pre></pre>	

AUTOMATED TESTING

- RequestFromL1(amount) (contra Reentrancy in L2VaulttransferToL1(uin External calls:	t256) (contracts/polygon/L2Vault.sol#540-553):
<ul> <li>bridgeEscrow.l2Withdraw(amoun Event emitted after the call(s)</li> <li>TransferToL1(amount) (contrac</li> </ul>	t) (contracts/polygon/l2Yault.sol#543) : fypolygon/l2Yault.sol#544)
Reentrancy in BaseVault.depositIntoStra External calls: - strategy.invest(tokenAmount)	tegy(BaseStrategy,uint256) (contracts/BaseVault.sol#323-339): (contracts/BaseVault.sol#337)
Event emitted after the call(s) - StrategyDeposit(strategy,toke Reentrancy in EmergencyWithdrawalQueue. External calls:	: Anount) (contracts/BaseVault.sol#338) dequeue() (contracts/polygon/EmergencyWithdrawslQueue.sol#79-94):
<ul> <li>redeemedAssetAmount = vault.r</li> <li>Event emitted after the call(s)</li> </ul>	edeemByEmergenyWithdrawalQueue.headBtr.withdrawalRequest.shares.withdrawalRequest.ecceiver.withdrawalRequest.owner) (contracts/polygon/EmergencyWithdrawalQueue.sol#85-87) i un(headBtr.withdrawalRequest.owner.withdrawalRequest.shares) (contracts/polygon/EmergencyWithdrawalQueue.sol#89-91) dequeueBath(intra56) (contracts/polygon/EmergencyWithdrawalQueue.sol#201)
External calls: - redeemedAssetAmount = vault.r	edeem8vEmergencvWithdrawalQueue(otr.withdrawalReguest.shares.withdrawalReguest.receiver.withdrawalReguest.owner) (contracts/polvgon/EmergencvWithdrawalQueue.sol#186-188)
Event emitted after the call(s) - EmergencyWithdrawalQueueDeque Reentrancy in L2WormholeRouter.receiveF External calls:	: en en headPtr,withdrawalRequest.comer,withdrawalRequest.receiver,withdrawalRequest.shares) (contracts/polygon/EmergencyWithdrawalQueue.sol#110-112) unds(bytes) (contracts/polygon/L2WorsholeRouter.sol#45-56):
- vault.bridgeEscrow().l2ClearE	und(amount) (contracts/polygon/L2WoreholeRouter.sol#54) : :acts/polygon/L2WoreholeRouter.sol#56) // . :acts/polygon/L2WoreholeRouters/BaseVault.sol#962-376):
– amountWithdrawn = strategy.di	vest(tokenAmount) (contracts/BaseVault.sol#364)
Event emitted after the call(s) - StrategyWithdrawal(strategy,a Reference: https://github.com/crytic/sl	: unutWihdrawn) (contracts/BaseVault.sol#374) ither/wiki/Detector-Documentation≢reentrancy-vulnerabilities-3
Dangerous comparisons:	racts/BaseVault.sol#407-662) uses timestamp for comparisons mestamp >= lastHisrvest + lockInterval,PROFIT_UNLOCKING) (contracts/BaseVault.sol#409)
<pre>Dangerous comparisons: - block.timestamp &gt;= lastHarves</pre>	mestamp >> lastHarvest = lockInterval,PROPT_UNLOCKING) (contracts/BaseVault.sol8409) vell.sol846-075/ uses timestamp for comparisons t + lockInterval (contracts/BaseVault.sol8469)
EmergencyWithdrawalQueue.dequeue() (con Dangerous comparisons:	tracts/polygon/EmergencyWithdrawelQueue.sol#79-94) uses timestamp for comparisons racts/polygon/EmergencyWithdrawelQueue.sol#88) //ZVuul.col#62-73 uses timestamp for comparisons
	n/L/Yault.sol#62-/3) uses timestamp for comparisons ts/polygon/L/Yault.sol#69) (unit256,unit26,uddress,dddress) (contracts/polygon/L2Yault.sol#200-236) uses timestamp for comparisons
Dangerous comparisons: - balanceOf(owner) < shares (co L2Vault.redeem(uint256,address,address)	euint20,uint20,adores,adores; (contract;/pojgdn/i/vauit.soi#20-/20) uses timestamp for comparisons ntracts/pojgdn/i2Vauit.sol#218) (contracts/pojgdn/i2Vauit.sol#23-274) uses timestamp for comparisons
Dangerous comparisons: - require(bool,string)(shares + L2Vault.withdraw(uint256,address,addres	emergencyWithdrawalQueus.debtToQuesr(owner) <= balanceQf(owner).Not enough share available in owners balance) (contracts/polygon/L2Vault.sol#240-243) 8) (contracts/polygon/L2Vault.sol#277-317) use timestamp for comparisons
Dangerous comparisons: - require(bool,string)(shares + L2VaultconvertToShares(uint256,L2Vaul	emergencyWithdramalOueus.debtroQuner(camer) <= balanceOf(camer),Not enough share available in camers balance) (contracts/polygon/L2Vault.sol#248-286) t.Rounding) (contracts/polygon/L2Vault.sol#348-353) uses timestamp for comparisons
	olygon/L2Vault.sol#344) t.Rounding) (contracts/polygon/L2Vault.sol#361-373) uses timestamp for comparisons
<ul> <li>totalShares == 0 (contracts/p L2Vault.lockedTVL() (contracts/polygon/</li> </ul>	olygon/L2Vault.sol#363) L2Vault.sol#468-475) uses timestamp for comparisons
<pre>- block.timestamp &gt;= lastTVLUpd L2Vault.detailedPrice() (contracts/poly Dangerous comparisons:</pre>	ate + lockInterval (contracts/polygon/L2Vault.sol#469) gon/L2Vault.sol#589-584) uses timestamp for comparisons
	p)ygon/L2Vault.sol#582) ithrz#wii/D#tector-Documentation#Dick-timestamp /estrans/Wullesl.sol#0-27) uses assembly
- INLINE ASM (contracts/externa Reference: https://github.com/crytic/sl	J/Wulficall.solft9-21) Infe/ski/JOpertor-Documentation#assembly-usage
	int256) (contracts/polypon/EmergencyWithdrawalQueue.sol#97-128) has costly operations inside a loop: polypon/EmergencyWithdrawalQueue.sol#83) (contracts/BaseVault.sol#246-271) has costly operations inside a loop: (contracts/BaseVault.sol#246-271) has costly operations inside a loop:
<ul> <li>maxLockedProfit += oldBal - a</li> <li>BaseVault.updateStrategyAllocations(Bas</li> <li>totalBps -= oldBps (contracts)</li> </ul>	ar (unitals/page/ault.olg/240-271) has costly operations inside a loop: mountifundramn (contract/SaevAult.solg/240-271) Skrateg()_units(solg/240-210) has costly coperations inside a loop: /BaevAult.solg/230] ract/SaevAult.solg/240-210) has costly operations inside a loop:
- totalBps = newTotalBps (contr	tract/SasVult.sol280=710 has costly operations inside a loop: act/SasVult.sol21209) ither/wiki/Detector-Documentation#costly-operations-inside-a-loop
BaseVaultassessFees() (contracts/Base L2VaultmsgData() (contracts/polygon/L Reference: https://github.com/crytic/s1	Vault.sol#531) is never used and should be removed ZVault.sol#22-129) is never used and should be removed Inter/ski/Decto-Concumstation/dead-code
Pragma version*0.8.13 (contracts/Affine Pragma version*0.8.13 (contracts/BaseSt	Governable.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rategy.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version^0.8.13 (contracts/BaseVa Pragma version^0.8.13 (contracts/Bridge Pragma version^0.8.10 (contracts/Consta Dragma version^0.8.12 (contracts/Wormho	ult_sol22) necessitates a version too recent to be trutted. Consider deploying with $0.4, 51/9, 7, 8/9, 8.7$ screws.sol21) necessitates a version too recent to be trutted. Consider deploying with $0.43/9, 7, 8/9, 8.7$ house sol21) necessitates a version too recent to be trutted. Consider deploying with $0.43/9, 7, 8/9, 8.7$ house sol210 necessitates and the screent to be trutted. Consider deploying with $0.43/9, 7/9, 8.7$
Pragma version*0.8.13 (contracts/interf	leBouter.sol#2) necessitates a version to recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 al/Mulricl1.sol#2) necessitates a version to recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 aces/IEBO4025.sol#2) necessitates a version to or recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version^0.8.13 (contracts/interf	aces/IRocIthaindenaper.col#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7 aces/IVuult.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7 n/Detailed.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7 n/Detailed.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7
Pragma version*0.8.13 (contracts/polygo	n/EmergencyWithdrawalQuue.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7 n/L2Wuit.sol#2) necessitates a version too recent tobe trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 n/L2WermblaGouter.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Reference: https://github.com/crytic/sl	line/wiki/Detoto-Documentation#incorrect-versions-of-solidity versil/ (control (versil) (w) tical) = of the -2014
- (success,result) = address(th Reference: https://github.com/crytic/sl	isl.delepsteell(data[i]) (contracts/external/Wulticall.sol#12) ither/wiki/Detector-Documentation#low-level-calls
Reference: https://github.com/crytic/sl	29-589) should isharit from ILZWalt (contracts/interfaces/IVault.sol#8-18) ither/wiki/Detactor-Documentation#missing-inheritance isa/www//Dwalt = a/dMA/L in/Dwalt (arthurs/in/Dwalt.col#80.580)
	ter (z. 1999) z. zakow zakow zakow zakow z zakow zakow z zakow zakow z zakow zakow z zakow zakow z zakow zakow z zakow zakow z zakow zakow z
Variable BaseVault.swapWithdrawalQueueI Variable Constants.L1_FUND_TRANSFER_REP Reference: https://github.com/crytic/s1	nderss(uint256,uint256,uint256,uint256,uint256,uint256,uint256,uint256,uint256,uint256,uint256).newStrategy2 (contracts/BaseVault.so GRT (contracts/Constants.solf2) is too similar to Constants.i2_FUD_TRANSFER_REPORT (contracts/Constants.solf7) Tuerfwiki/Detect-PocumentsIonWarable-news-are-too-cimilar
BaseStrategy (contracts/BaseStrategy.so - BaseStrategy.balanceOfAsset() - BaseStrategy.divest(uint256)	12F-40 does not (splemant functions: (contract/BacKstady.al/22) (contract/BacKstady.al/26) (contract/BacKstatey.al/26)
<ul> <li>BaseStrategy.totalLockedValue</li> </ul>	(unitativ/absolitatoy.sol/d0) () (contract/Bassitatoy.sol/d0) () fier/ski/Detect-Documentation/uninglemented-functions
	geEscrow.sol#19) should be constant ther/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
asset() should be declared external: - BaseVault.asset() (contracts/ - L2Vault.asset() (contracts/po	Base/Sault.sol/#39-35)
<pre>multicall(bytes[]) should be declared e</pre>	<pre>xternal: (contract;/wulticall.sol#9-27) ternal:</pre>
<ul> <li>EmergencyWithdrawalQueue.link</li> <li>totalDebt() should be declared external</li> <li>EmergencyWithdrawalQueue tota</li> </ul>	Vallt(IVault) (contracts/objyon/EmergencyWithdrawalQueus.ol#46-57) hoh() (contracts/objyon/EmergencyWithdrawalQueus.ol#46-57)
initialize(address,ERC20,address,Bridge - L2Vault.initialize(address,ER convertToShares(uint256) should be decla	Escrom, HenegencyWithdramalQueue, address, uint256, uint256/2/) should be declared external: C20, address, 8ridgeEscrue, EnergencyWithdrawalQueue, address, uint256, uint256/2/) (contracts/polygon/L2Vault.sol#83-110) red arternal:
<pre>convertToAssets(uint256) should be decl:</pre>	6) (contracts/polygon/L2Vault.sol#35-337) red attarn1: 50) (contracts/polygon/L2Vault.sol#356-358)
maxDeposit(address) should be declared ( - 12Vault.maxDeposit(address) (	) (contracts/polygon/L2Yault.sol#391-393) pretraits pretraits/nolymon//2Yault.sol#39-416)
<pre>maxMint(address) should be declared ext - L2Vault.maxMint(address) (con maxRedeem(address) should be declared ex</pre>	zral: tracts/polygon/L2Vault.sol#419-422) ternal:
<ul> <li>L2Vault.maxRedeem(address) (cr maxWithdraw(address) should be declared</li> </ul>	ontracts/polygon/L2Vault.so1#425-427)
	about the Debugger of the West of the West of the Annual Annual Annual Annual Annual Annual Annual Annual Annual

### src/polygon/ERC4626Router.sol

- sll.multicall(bytes[]) (contracts/external/Multicall.sol#9-27) uses assembly TNLIME ASM (contracts/external/Multicall.sol#9-21) nos: https://github.com/rytic/silther/miki/Dotector-Documentation#assembly-usage
- Pragma version\*8.8.13 (contracts/external/Multical1.sol#4) necessitates a version too recent to be trusted. Consider deploying mith 8.6.12/8.7.6/8.8.7 Pragma version\*8.8.13 (contracts/interface/IERO4626.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.8.7 Pragma version\*8.8.13 (contracts/polygon/EKO4620Router.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.8.7 Pragma version\*8.8.13 (contracts/polygon/EKO4620Router.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.8.7
- or deployment ytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

### src/polygon/ERC4626RouterBase.sol

- ulticall(bytes[]) (contracts/external/Multicall.sol#9-27) uses assembly NRINE ASM (contracts/external/Multicall.sol#19-21) https://dibub.com/crvii/claitae/wiki/desterna-borumentation#assembly-
- ersion%0.8.13 (contracts/axternal/Multicall.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 ersion%0.8.13 (contracts/interfaces/IEEGC426.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 ersion%0.8.13 (contracts/oploying/REG42640artBase.sol#1) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
- loyment lither/wiki/Detector-Documentation#incorrect-versions-of-solidity

### src/polygon/Forwarder.sol

versint%.8.13 (contracts/polygom/forwarder.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.7 1.16 is not recommended for deployment s: https://github.cod/crytics/libiter/wiki/Detector-Documentation#incorrect-versions-of-soligity

#### src/polygon/L2AAVEStrategy.sol

Multicall.multicall(bytes[)) (contracts/external/Multicall.sol#9-27) has delegatecall inside a loop in a payable function: (success,result) = address(this).delegatecall(data[i)) (contracts/external/Multicall.sol#12 Reference: https://github.com/crytis/slither/wiki/Detector=Documentation/#payable=functions-using=delegatecall=inside=a-loop
AffindBovernable.governamce (contracts/AffineBovernable.sol#6) is never initialized. It is used in: NormbiBhouter.other.symphoter [contracts/NormbiBhouter.sol#3] is never initialized. It is used in: NormbiBhouter.other.symphoter [contracts/NormbiBhOuter.sol#3] is never initialized. It is used in: - NormbiBhouter.vildstewormbleBhouter.sol#3]
<pre>BaseAult.reblance() (contract/BaseAult.solf640-590) uses a damperous trict equality:</pre>
Reentrumy im BaseVault.harvest(BaseStrategy(]) (contracts/BaseVault.sol#407-462): Externel calls: - balancofhisHarvest = strategy,totallookesVaul() (contracts/BaseVault.sol#432) State variables writen after the call(s): - strategiss(itrategy).balance = balancsFhisHarvest (contracts/BaseVault.sol#435) Reference: https://github.com/grit/siltertest/comunistionFarestalIntary=valuesballities-1
BasYault_screpnizedithdrawalQowum().cffset(contracts/BasYault.so/E229) is a local variable newer initialIzed BasYault_teblamce],anountsFinwati (contracts/BasYault.so/E656) is a local variable newer initialIzed BasYault.harvest(BasSEtategy()).totsJProfifscruwd (contracts/BasYault.so/E6408) is a local variable newer initialIzed Reference: http://github.com/group/sit/Sutterformation/sites/BasYault.so/E6408 is a local variable newer initialIzed
BaseYoult:rtblane().(contracts/BaseYoult.sol8569-500) ignores return value by strategy.rdiset(curStrategyTVL) (contracts/BaseYoult.sol8557) L2AMEStrategyelinatAmetricate/pipegr/L2AMEStrategy.sol8120-130) ignores return value by incentivesController.classBewards(getAweAssatt), type()(uin726) inae,address(sters(his)) (contracts/polygon/L2AMEStrategy.sol8120-130) ignores return value by incentivesController.classBewards(getAweAssatt), type()(uin726) inae,address(sters(his)) (contracts/polygon/L2AMEStrategy.sol8120-130) ignores return value by incentivesController.classBewards(getAweAssatt), type()(uin726) inae,address(his)) (contracts/polygon/L2AMEStrategy.sol8120-130) ignores return value by incentivesBevards(getAweAssatt), type()(uin726) ignores return value by incentivesBe
BaseVault.baseInitialize(address,ERC20,address,BridgeEscrow)governance (contracts/BaseVault.sol#87) lacks a zero-check on : - governance = _governance (contracts/BaseVault.sol#2) BaseVault.baseInitialize(address,ERC20,address,BridgeEscrow),wormholeBouter (contracts/BaseVault.sol#37) lacks a zero-check on : - wormholeBouter = _wormholeBouter (contracts/BaseVault.sol#4) BridgeEscore.comstructer(address)worm(contracts/BaseVault.sol#4) BridgeEscore.comstructers/BridgeEscore.sol#20] lacks a zero-check on :
<pre>- ownet = _ownet (contract/BridgeEscow.olB29) FidgeEscow.initialstatedmeest, Noothankawaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</pre>
<pre>- resultation = resultation (contracts/polygon/L2AWEStrategy.sol#63) L2AWEStrategy.constructor(BaseVulls,Address,Address,Address,, varappedMative (contracts/polygon/L2AWEStrategy.sol#49) lacks a zero-check on :</pre>
<pre>Multicall(prise()) (contracts/steeral/Multicall.sol#0-27) has stermal calls inside a loop: (success, result) = address(his) adlepstcall(dist(i)) (contracts/steeral/Multicall.sol#02) BeseNult.reveSteregy(BeseNettaregy(Bese</pre>
Reentrancy in BaseVault.removeStrategy(BaseStrategy) (contracts/BaseVault.sol#240-271):

: wm = strategy.divest(type()(uint256).max) (contracts/BaseVau s written after the call(s): Fit += oldBal - amountWithdrawn (contracts/BaseVault.sol#267) Holdings = oldBal (contracts/BaseVault.sol#259)

Reentrancy in BaseYault.withdrawFromStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#362-376): External
- amountWithdrawn = strategy.divest(tokenAmount) (contracts/BaseVault.sol#364)
State variables written after the call(s): - strategis[stratgy].balnoe == asunWithdram (contracts/BaseYault.sol#366)
<ul> <li>totalStrategyholdings == amouthithdrawn (contracts/dssvault.sgl#37)</li> <li>Referencis Https://github.com/grtis/olithers/wiki/Betector-Documentariong=wollnerabilities=2</li> </ul>
Reentrancy in BaseVault.depositIntoStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#323-339):
External calls: - strategy.invest(ckenAmount) (contracts/BaseYault.sol#337)
Form smitted after the call(s): - StartegyDeposit(startegy,tokankount) (contracts/BaseVault.sol#338)
Reentrancy in BaseVault.withdrawFromStrategy(BaseStrategy,uint256) (contracts/BaseVault.so1#362-376):
External calls: - assurbithdram = strategy.divest(tokenAmount) (contracts/BaseVault.sol#364)
Event emitted after the call(s): - StrategyWithdmawNifkategy,mountWithdmawn) (contracts/BaseVault.sol#374)
BaseNult.harvest(BaseStrategy()) (contracts/BaseVault.sol#487-642) uses timestamp for comparisons Dangerus comparisons
- require(boo), string) (block, timestamp >= lastHarvest + lock/interval, PROFT_UMLOOCHNO) (contracts/BaseYault.sol#4849) BaseWault.lock#Proft() (contracts/BaseYault.sol#484-75) use stimestamp for comparison (contracts/BaseYault)
Dangerous comparisons:
<ul> <li>block:timestmp&gt;=lastMarsest = lockIntersval(contracts/MarsVull.solP469)</li> <li>Persence: http://glubu.com/cyriic/silters/vull.solP469</li> </ul>
Multicall.multicall(bytes()) (contracts/external/Multicall.sol#9-27) uses assembly
- INLINE ASM (contracts/sternal/Multicall.soll59-23) Perference: https://dithub.com/cyriis/silter/sterna/si/Detector-documentation#ssembly-usage
BaseYault.removeStrategy(BaseStrategy) (contracts/BaseYault.sol#240-271) has costly operations inside a loop:
- totalRos -= stratInfo tvlRos (contracts/RaseVault_sol#268)
BaseVault.removsStrategy(BaseStrategy) (contracts/BaseVault.sol#240-271) has costly operations inside a loop: - totalStrategy(BaseStrategy) (entracts/BaseVault.sol#259) BaseVault.removStrategy(BaseStrategy) (entracts/BaseVault.sol#249-77) has costly operations inside a loop:
na anticked#rof1:== oldbl=_esountHithdram (contract/Baravallt.sol2207) Baskvalt.upd#rof2:== oldbl=_esountHithdram (contract/Baravallt.sol2207) Baskvalt.upd#rof2:== oldbl=_esountBaravallt.sol2207 bas contly operations inside a loop:
- totalBps -= oldBps (contracts/BaseVault.sol#293)
BaseVault_increassTVEBps(uint256) (contracts/BaseVault.sol4286-120) has costly operations inside a loop: - totalBps enmotfalBps (contracts/BaseVault.sol2200)
Reference: http://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop
BaseVault_pliquidate(uint256) (contracts/BaseVault.s.ol#964-525) is never used and should be removed BaseVault_depositIntOstrategies() (contracts/BaseVault.sol#864-535) is never used and should be removed
BaseNault.depoilt.ne55trsteg/BaseStrategy.uint256) (contracts/BaseNault.ac0823-339) is never used and shuld be removed BaseNault.sth/stareForstrategy(BaseStrategy.uint256) (contracts/BaseNault.ac0826-378) is never used and should be removed
WormhollABuuter, validsteVormhollAMessaphäitisef(NormhollAButer, soläd1-46) is never used and should be removed Reference: https://dithub.com/criti/althuter/solad-code
Martinet (1,1) (contractive) for a second
Pragma version^0.8.13 (contracts/BaseStrategy.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version*8.1.3 (contracts/BaseYull.sol42) necessitates a version too recent to be trusted. Considerd opploying with 8.4.312(0.7.6/8.8.7) Pragma version*8.1.31 (contracts/BridgeStorws.0.120) necessitates a version too recent to be trusted. Consider deploying with 8.4.312(0.7.2/8.7.6)
Pragma version 8.1.3 (contracts/hormholeRoutes.sol23) necessitates a version too recent to be trutted. Consider deploying with 0.4.12/0.7.6/0.8.7 Pragma version 8.1.3 (contracts/hormholeRoutes.lall.sol4), horesistates a version too recent to be trutted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version^0.8.13 (contracts/interfaces/IRootChainManager.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version% 8.13 (contracts/interfaces/Unilks@MapBouter.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 Pragma version% 8.13 (contracts/interfaces/IVault.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.13 (contracts/interfaces/IVault.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version^0.8.13 (contracts/interfaces/aave/IAToken.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version% 8.13 (contracts/interfaces/ave/IAswe/InterColler.solf2) necessitates a version to recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7 Pragma version% 8.13 (contracts/interfaces/ave/InitializablaCoken.solf2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7
Pragma version 4.1.3 (contracts/interfaces/ase/IlendingPoll.sol#2) mecessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version 48.1.3 (contracts/interfaces/ase/IlendingPolladdresseProvides.col#2) executo to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version*8.1.3 (contracts/interfaces/ame/fiSeialeBalanceTeken.sal2) necessitates a version to necent to be trusted. Consider deploying with 8.4.3(20.7.6/0.8.7 Pragma version*8.1.3) (contracts/polypen/12AMEStratego,sal2) necessitates a version to necent to be trusted. Consider deploying with 8.4.37(2.7.6/0.8.7
Progma version/6.11[1]/drat/pres.es/82] necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 soli-0.8.16 in tercommended for deployment
Kals-es.io 15 not récommende tro équipyment Reference: https://github.com/cryit/s/lither/wiki/Detector-Documentation#incorrect-versions-of-solidity
<pre>Low lawel call in Multicall.inditicall.inditicall.inditicall.inditectall.inditicall.inditicall.inditicall.inditicall.inditicall.inditicall.inditicall.inditicall.inditicalli.inditica</pre>
- (SOCES, (ESI)/ = ADDESS((NS)/GOLDES((IGATI))) Reference: http://pithuk.com/pit/c/lither/wiki/Detecto-DocumenticalPite=leel-eals
Variable BaseVault.swapWithdrawalQueueIndexes(uint256,uint256).newStrategy1 (contracts/BaseVault.so) Reference: https://github.com/crytic/slither/wiki/Betector-Bocumentation#variable-names-are-too-similar
BridgeScree, vultimer (contract/SridgeScree, soll) should be constant 20XMSStratey.vultimers(Contract/SridgeScree, soll29) should be constant
WormholeRouter.nextValidNonce (contracts/WormholeRouter.sol#15) should be constant
WormholRouter.etherLayerChainId (contract/WormholRouter.solfA) should be constant WormholRouter.sohrtayerOuter (contract/WormholRouter.solf3) should be constant
asse() should be declared external: - Besevalut.asse() (contracts/BaseVault.scl#33-35)
basefnitialize(address, RFC29, address, RFC29,

# src/polygon/L2Vault.sol

	ategy.vault (contracts/BaseStrategy.sol#13) is - BaseStrategy.sweep(ERC20) (contracts/BaseStr	never initialized. It is used in: targy.sol243-47) never initialized. It is used in: atogy.sol24-47) ctor-Documentation#uninitialized-state-variables
	<pre>ategy.asset (contracts/BaseStrategy.sol#21) is - BaseStrategy.sweep(ERC20) (contracts/BaseStr - Contracts/BaseStr</pre>	never initialized. It is used in: stay, solid-2-7)
L 2Vault	<pre>ce: https://github.com/crytic/siither/wiki/bete assessEees() (contracts/polycom/12Vault_sol#6</pre>	ctor-upcumentationsuminitalize-state-states
czradze.	<pre>-feesBps = (duration * managementFee) / SECS_P -numSharesToMint = (feesBps * totalSupply()) /</pre>	2-33) performs a multiplication on the result of a division: RryAR(contrats/polypon/LYAULt.solA65) MX_ABS(contrats/polypon/LYAULt.solA67) cto-DocumentarionAdvide=barGer=multiply
Referenc	ce: https://github.com/crytic/slither/wiki/Dete	cto-Documentation#divide-before-multiply
L2Vault.	<pre>assessFees() (contracts/polygon/L2Vault.sol#6 - numSharesToMint == 0 (contracts/polygon/L2Va</pre>	2-73) uses a dangerous strict equality: uit:sol2007 sol2004 sol
L2Vault.	<pre>convertToAssets(uint256,L2Vault.Rounding) (co - totalShares == 0 (contracts/polygon/L2Vault.</pre>	ntracits/polygon/L2Vault.sol#361-373) uses a dangerous strict equality:
L2Vault.	convertToShares(uint256,L2Vault.Rounding) (co - totalShares == 0 (contracts/polygon/L2Vault.	ntraets/polygon/L2Vault.sol#348-353) uses a dangerous strict equality: sol#34A)
BaseVau]	<pre>lt.rebalance() (contracts/BaseVault.sol#549-598</pre>	) uses a dangerous strict equality: mB&A/
L2Vault.	<pre>.receiveTVL(uint256,bool) (contracts/polygon/L2 - delta == 0 (contracts/polygon/L2Vault.sol#50</pre>	Vault.sol#477-586) uses a dangerous strict equality:
Reentrar	<pre>https://www.indrawaiQueue.dequeue() (cont External calls: </pre>	racts/polygon/ExergencyWithdrawalQuuue.sol#79-44): yWithdrawalQuuue(headPtr,withdrawalRequest.shares,withdrawalRequest.receiver,withdrawalRequest.ommer) (contracts/polygon/ExergencyWithdrawalQuuue.sol#85-87) hdrawalQuuue.sol#847 acts/BaseYauit.sol#487-462):
	<pre>State variables written after the call(s):</pre>	yn thu an agunu hann ty at hu an an hugust, saar sy at hu an an hugust, ac beret, a thu an an hugust, om sy'r t Harnel Dunne o 1803
Reentrar	<pre>ncy in BaseVault.harvest(BaseStrategy[]) (contr External calls:</pre>	acts/BaseVault.sol#407-462):
	- balanceThisHarvest = strategy.totalLockedVal State variables written after the call(s):	(contracts/BaseVault.sol#432)
Referenc	- strategies[strategy].balance = balanceThisHa ce: https://github.com/crytic/slither/wiki/Dete	us() (contracts/BaseWault.sol4432) rvsst (contracts/BaseWault.sol4435) curo-Documentation#reentrancy-wilmerabilities-1
BaseVau]	lt.harvest(BaseStrategy[]).totalProfitAccrued (	contracts/BaseVault.sol#418) is a local variable never initialized
BaseVaul L2Vault	ltorganizeWithdrawalQueue().offset (contracts computeRebalance().invest (contracts/polygon/	/BaseVault.sol#219) is a local variable never initialized L2Vault.sol#510) is a local variable never initialized
BaseVau] Referenc	lt.rebalance().amountsToInvest (contracts/BaseV ce: https://github.com/crytic/slither/wiki/Dete	contracts/BaseVault.sol#438) is a local variable never initialized /BaseWault.sol#219 is a local variable never initialized /ZVault.sol#219 is a local variable never initialized Ault.sol#560 is a local variable never initialized tor=Documentationuminitialized-local-variables
BaseVau]	lt.rebalance() (contracts/BaseVault.sol#549-590	) ignores return value by strategy-divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol8567) acts/plygon/L2WormholeRouter.sol295-03 ignores return value by wormhole.publishMessage(uin132(sequence),paylosd,consistencyLevel) (contracts/polygon/L2WormholeRouter.s gon/L2WormholeRouter.sol295-041 ignores return value by wormhole.publishMessage(uin132(sequence),paylosd,consistencyLevel) (contracts/polygon/L2WormholeRouter.s disc-DocumentationAunused-return
L2Wormho Reference	pleRouter.requestFunds(uint256) (contracts/poly ce: https://github.com/crytic/slither/wiki/nate	gon/L2WormholeRouter.sol#36-41) ignores return value by wormhole.publishMessage(unt32(sequence),payload,consistencyLevel) (contracts/polygon/L2WormholeRouter.s cor=Documentation#unused-return
	<pre>- governance = _governance (contracts/BaseVaul ce: https://github.com/crytic/slither/wiki/Dete</pre>	scrom) (contracts/BaseVault.sol#37-64) should emit an event for: t.sol#42; tot-Documentation#missing-events-access-control
	.setManagementFee(uint256) (contracts/polygon/L	2Vault.sol#54-56) should emit an event for:
	<ul> <li>withdrawalFee = feeBps (contracts/polygon/L2 .initialize(address,ERC20,address,BridgeEscrow,</li> </ul>	Vault.sol#59) EmergencyWithdrawalQueue,address,uint256,uint256(z)) (contracts/polygon/L2Vault.sol#83-110) should emit an event for:
	<ul> <li>- IlRatio = _llRatio (contracts/polygon/L2Vaul</li> <li>- l2Ratio = _l2Ratio (contracts/polygon/L2Vaul</li> </ul>	t.sol#100) t.sol#101) (V.d.a.sl00)
1.21/1	<ul> <li>withdrawalFee = fees[0] (contracts/polygon/L</li> <li>managementFee = fees[1] (contracts/polygon/L</li> <li>contracts/polygon/L</li> </ul>	Vaultsol856) Vaultsol85640 should emit an event for: EmergencyXithdrawalQueue,address,uint256,uint256,uint256[2]) (contracts/polygon/L2Vault.sol#83-110) should emit an event for: t.sol#1801) Zvult.sol1480] Zvult.sol1480 Zvult.sol1480-452) should emit an event for:
czvaurt.	- llRatio = _llRatio (contracts/polygon/L2Vau)	ygun zerozerisorine, nozy should emit an event roz: t.so[4450) t.so[451]
	<ul> <li>IRatio = _lRatio (contracts/polygon/L2Vau)</li> <li>1Ratio = _lRatio (contracts/polygon/L2Vau)</li> <li>1Ratio = _l2Ratio (contracts/polygon/L2Vau)</li> <li>maxlockedTVL = lockedTVL() + totalProfit (co</li> </ul>	Vault.sol4477-560) should emit an event for: httacts/polygon/(2Vault.sol4497)
	<pre>- LiTotalLockedValue = tvl (contracts/polygon/ ce: https://github.com/crytic/slither/wiki/Dete</pre>	L2Yault.sol#499) ctor-Documentation#missing-events-arithmetic
	- owner - owner (contracte/BridgeEscr	
	<pre>- vault = _vault (contracts/BridgeEscr - wormholeRouter = BaseVault(_vault).w</pre>	ow,sol385) ornhol#Router() (contracts/BridgeEscrow.sol#36)
BaseVau]	<pre>lt.baseInitialize(address,ERC20,address,BridgeE</pre>	orshol@kolter() (contracts/BridgeEscrow.sol283) scrow)_govername (contracts/BaseVault.sol937) lacks a zero-check on : BaseVault.eld/2)
BaseVaul	<pre>lt.baseInitialize(address,ERC20,address,BridgeE</pre>	scrow), wormholeRouter (contracts/BaseVault.sol#87) lacks a zero-check on : ntracts/BaseVault.sol#44) unitals,_cherLayerRouter (contracts/polygon/L2WormholeRouter.sol#18) lacks a zero-check on :
Lawormno	<pre>- otherLayerRouter = _otherLayerRouter</pre>	untus), _cnretusyerwours (contracts/polygon/Lzwommolakouter.sol#ls/ lacks a zero-cneck on : (contracts/polygon/L2WomholeRouter.sol#25) cot-Documentation#missing-zero-address-validation
Emergen		
	cyWithdrawalQueue.dequeueBatch(uint256) (contra (contracts/polygon/EmergencyWithdrawalQueue.so	cts/polygon/EmergencyWithdrawalQueue.sol#07-120) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawalQueue(ptr,withdrawalRec 1#f80-1001 1#f100-1001
	cyWithdrawalQueue.dequeueBatch(uint256) (contra (contracts/polygon/EmergencyWithdrawalQueue.so	cts/polygon/EmergencyWithdrawalQueue.sol#97-128) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawalQueue(ptr,withdrawalRec 1#186-1881 Wull sol#242-231 has external calls [arids a loop: mountWithdrawn = stateway disarf(zmed)(with264) ase) (contract/BaseNoult sol#267)
	cyWithdrawalQueue.dequeueBatch(uint256) (contra (contracts/polygon/EmergencyWithdrawalQueue.so	cts/polygon/EmergencyWithdrawalQueue.sol#97-128) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawalQueue(ptr,withdrawalRec 1#186-1881 Wull sol#242-231 has external calls [arids a loop: mountWithdrawn = stateway disarf(zmed)(with264) ase) (contract/BaseNoult sol#267)
BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul Multical	cyclibitizmalünaus dapanamätetkiinitääs) (contra contractizyo joyn / kavancyviitäänsa Dauma sa La navos kirastayu (Baskiratny) (contracta Maski La navos kirastayu (Baskiratny) (contracta Maskirat La navos kirastayu (Daskiratny) (contracta Maskiratny) La navos kirastayu (Contracta Maskiratny) La nabalanci (Contracta Maskiratny) La nabal	<pre>tit(pDignofBergencyWithdrawelQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawelQueue(ptr,withdrawelRec 1868-180) VullseD240-271) has external calls inside a loop: amountWithdrame = xrategy_dives(type(((unit26),wang)(contracts/Besafualt.sol#257) .sol#267-463) has external calls inside a loop: amountWithdrame = xrategy_dives(type(((unit26),wang)(contracts/Besafualt.sol#257) .sol#267-463) has external calls inside a loop: amountGinest, asset.balance0f(addres(this)) (contracts/Besafualt.sol#253) ) has external calls inside a loop: attrategy_comp_livestime.tamontToinvest() (contracts/Besafualt.sol#268) ) has external calls inside a loop: attrategy_comp_livestime.tamontToinvest() (contracts/Besafualt.sol#268) ) has external calls inside a loop: attrategy_trategy_tratesetWitheod() (contracts/Besafualt.sol#268) ) has external calls inside a loop: attrategy_tratesetWitheod() (contracts/Besafualt.sol#268) ) has external calls inside a loop: (success,result) = addresetWith() (doptateset/Besafualt)() (contracts/Besafualt.sol#267) callsol#2-77) has external calls inside a loop: (success,result) = addresetWith() (doptateset/System1/Auticall.sol#20)</pre>
BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul Multical Reference	cyhithdrawalQuuus.deguusBath(uint26) (contra (contrats/polygon/EmrgencyhithdrawalDurus.os (tontrats/polygon/EmrgencyhithdrawalDurus.os (tontrats/polygon/EmrgencyhithdrawalDurus/Basevall. 1:rebalance() (contrats/Basevall.sol856-590 1:rebalance() (contrats/Basevall.sol856-590 1:rebalance	<pre>cts/polygon/EmergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawslQueue(ptr,withdrawslRec Laigo-120) Laigo-120) &gt; as external calls inside a loop: mountWithdrawn = xtrategy.divest(type(](uint260.asa) (contracts/BaseVault.sol#57) &gt; as external calls inside a loop: sunsetfinitewrest = strategy.totallocdedVault.col#457) &gt; has external calls inside a loop: sunsetfinitewrest = strategy.totallocdedVault.col#457) &gt; has external calls inside a loop: surstays_comps.investingenviteWithdrawnlCommuterStateWault.col#583) &gt; has external calls inside a loop: surstays_comps.investingenviteWithdrawnlCommuterStateWault.sol#583) &gt; has external calls inside a loop: surstays_comps.investingenviteWithdrawnlCommuterStateWithdrawslCommuterStateWithdrawnlCommuterStatesWithdrawnlCommuterStateWithdrawnlCommuterStatesWithdrawnlCommuterStatesWithdrawnlCommute</pre>
BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul Multical Reference Reentrar	cyhihdrawalQueus.dequeuBath(uint250) (contra (contrati/polygor/EergencyhihdrawalQueus.so 1. convertantegor/Georgi1190) (contrati/polygor/Eergencyhi 1. robalanee() (contrati/Barvul.sol556-969 1. robalanee() (contrati/Barvul.sol566-969 1. rob	<pre>cts/polygon/EmergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawslQueue(ptr,WithdrawslRec Litdo-180) Litdo-180 NaukAdM-463 has external calls inside a loop: amountWithdrawn = strategy_dives(type(1(sint26),sas)(centracts/Base/ault.sol#257) NaukAdM-464 has external calls inside a loop: amountWithdrawn = strategy_dives(type(1(sint26),sas)(centracts/Base/ault.sol#257) Na external calls inside a loop: strategy_comp.linvestintamountToInvest, asset.balanceOf(address(this)) (contracts/Base/ault.sol#258) ) has external calls inside a loop: strategy_comp.linvestintamountToInvest, asset.balanceOf(address(this)) (contracts/Base/ault.sol#568) ) has external calls inside a loop: strategy_comp.linvestintamountToInvest() (contracts/Base/ault.sol#568) ) has external calls inside a loop: strategy_totallockedValue() (contracts/Base/ault.sol#567) call.sol#2-27) has external calls inside a loop: success,teault) = address(this).delegatecall(dats[]) (contracts/external/Multicall.sol#12) ttracts/polygon/L2Vault.sol#527-538):</pre>
BaseVau BaseVau BaseVau BaseVau BaseVau BaseVau Multica Reference Reentran	<pre>cpditdramalDuce.dourseBatch(int26) (contr (contractpr)ppd(mergerupp)(topres)(contractpr) (contractpr)ppd(mergerupp)(topres)(contractpr) (contractpr))(contractpr)(contractpr) (contractpr)(contractpr)(contractpr)(contractpr) (contractpr)(contractpr)(contractpr)(contractp) (contractpr)(contractpr)(contractpr)(contractp) (contractpr)(contractpr)(contractpr)(contractp) (contractpr)(contractpr)(contractpr)(contractpr) (contractpr)(contractpr)(contractpr)(contractpr) (contractpr)(contractpr)(contractpr)(contractpr)(contractpr) (contractpr)(contractpr)(contractpr)(contractpr)(contractpr) (contractpr)(c</pre>	<pre>tit(/Diggn/SmergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawslQueue(ptr,withdrawslRec 1848-148) Vull:sol#244-271) has external calls inside a loop: mountWithdramn = strategy.divest(type(((uint26).max)(contracts/BaseVault.sol#257)) .sol#264-261) ) has external calls inside a loop: amountWithdramn = strategy.divest(type(((uint26).max)(contracts/BaseVault.sol#257)) .sol#264-261) has external calls inside a loop: strategy.compl.shunetMithdramn = strategy.divest(type(((uint26).withdrams)(contracts/BaseVault.sol#257)) ) has external calls inside a loop: strategy.compl.ivest(contracts/BaseVault.sol#258) ) has external calls inside a loop: (success, result) = ddrass(this).delgatecali(dsts[i]) (contracts/external/Multicall.sol#12) ctor-Documentation/ecalls.inside a loop: (success, result) = ddrass(this).delgatecali(dsts[i]) (contracts/external/Multicall.sol#12) ntracts/polygon/L2Vault.sol#257-538): t.ol#2531</pre>
BaseVau BaseVau BaseVau BaseVau BaseVau BaseVau Multica Reference Reentrar	optith@samplones.degramalth(in1256).contr (contrat(p))(p)(fmspreped)(b)(trasplowe).a tromosofirstopy(lassifratop)(contrats/hese tromosofirstopy(lassifratop)(contrats/hese tromosofirstop)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 tromalance)(contrats/hese/ul.sal564-090 from for the tromal tromal tromal tromal for the tromal tromal tromal tromal tromal for the tromal tromal tromal tromal tromal for the tromal transformed tromal tromal tromal - bridgeterom lattithera (assumt) (contrats/hese(assumt)(contrats/hese(assumt)) - bridgeterom lattithera (assumt)(contrats/hese(assumt)(contrats/hese(assumt)))	<pre>tid/pDigon/EmergencyWithdrawelQueue.sol#77-120) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawelQueue.ptr,withdrawelRec L#86-189) Vault.sol#240-731) has external calls inside a loop: mountWithdrawe = strategy_divest(type((usint26),ama)(contracts/BaseVault.sol#257) .sol#247-463) has external calls inside a loop: mountVithdrawe = strategy_divest(type((usint26),ama)(contracts/BaseVault.sol#257) .has external calls inside = loop: mountVithdrawe = strategy_divest(type((usint26),ama)(contracts/BaseVault.sol#257) .has external calls inside = loop: trategy_comp_l.invest(amountFinnest) (contracts/BaseVault.sol#260) .has external calls inside = loop: trategy_comp_l.invest(amountFinnest) (contracts/BaseVault.sol#267) .has external calls inside = loop: (success,result) = addres(this).delegatecall(data(i)) (contracts/external/Multicall.sol#12) ctor=DocumentAtion#external_sol#267-538): t.sol#531 .tosl#531 .tosl#531 .tosl#531</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Reference Reentrar	<pre>cptitdramalDuos.depuesBath(Lint26) [contr [contEntralph]ppd[Emspurch]thdramalDuosa.so [contEntralph]ppd[Emspurch]thdramalDuosa.so [contEntralph][contEntralph][contralph] [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance] contrats/3msvul.sol654-090 [restrict] contrats/3msvul.sol654-090 [restrict] contrats/3msvul.sol654-090 [trabalance] contrats/3msvul.sol64-090 [restrict] contrats/3msvul.sol64-090 [restrict]</pre>	<pre>tit(/Diugon/BergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawslQueue(ptr,withdrawslQueu</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Reference Reentrar	<pre>cptitdramalDuos.depuesBath(Lint26) [contr [contEntralph]ppd[Emspurch]thdramalDuosa.so [contEntralph]ppd[Emspurch]thdramalDuosa.so [contEntralph][contEntralph][contralph] [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance(] contrats/3msvul.sol654-090 [trabalance] contrats/3msvul.sol654-090 [restrict] contrats/3msvul.sol654-090 [restrict] contrats/3msvul.sol654-090 [trabalance] contrats/3msvul.sol64-090 [restrict] contrats/3msvul.sol64-090 [restrict]</pre>	<pre>tit(/Diugon/BergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawslQueue(ptr,withdrawslQueu</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Reference Reentrar	<pre>cpditdexalbus.deguadath(init26) (conta (creased raby) (develop()) (contact/hese) (creased raby) (develop()) (contact/hese) (creased raby) (develop()) (contact/hese) (creased raby) (contact/hese) (creased raby) (creater/hese) (creased raby) (creater/hese) (creased raby) (creater/hese) (creased raby) (creater/hese) (creased raby) (creased raby) (creased raby) (creased raby) (creased raby) (creased raby) (creased raby) (creased raby) (</pre>	<pre>tt/polgon/EmergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawslQueue(ptr,withdrawslQueue</pre>
BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul Multical Reference Reentrar	<pre>cptitdramalQueue.dequeuBath(uint26) (contrat (contratt polygon/GergencydithdramalQueue.so (contratt polygon/GergencydithdramalQueue.so (threat) (contratt/SaseVult.sol654-050 11 rebalance() (contratt/SaseVult.sol654-050 1 rebalance() (contratt/SaseVult.sol654-050 iconficient) (contratts/SaseVult.golf) iconficient) (contratts/SaseVult.golf) contraft[cials(contrats/SaseVult.gol</pre>	<pre>ttr/plugn/EmergencyWithdrawslQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdrawslQueue(ptr,withdrawslQueue</pre>
BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul Reference Reentrar	optithese longer degramment this initial (contra (contrativhous) of despression links and longer it removes that the links of the links and longer it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the links of the links of the links it removes the links of the link	<pre>trt/plugn/fmergencyWithdramelQueue.sl#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdramelQueue(ptr,withdramelReec Wint 100 000 000 000 000 000 000 000 000 000</pre>
BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul BaseVaul Reference Reentrar	opiinkaaalbuma daguamahthikint260 (contr (contratifo)upii faragpiceybii (contratifo)upii faragpiceybii (contratifo)upii faragpiceybii (contratifo)upii faragpiceybii (contratifo)upii (contratifore) (con	<pre>trid/polypon/fmergencyWithdramelQueue.sol#77-120) has external calls inside a loop: redeemedAssetAnount = vault.redeemByEmergencyWithdramelQueue(ptr,withdramelRec ims6-169) Vault.sol#240-711 has external calls inside a loop: mountWithdrame = strategy.divest(type()(uint26).max)(contracts/BaseVault.sol#257) .sol#247-463) has external calls inside a loop: mountWithdrame = strategy.divest(type()(uint26).max)(contracts/BaseVault.sol#257) .hs external calls inside = loop: mountVithdrame = strategy.divest(type()(uint26).max)(contracts/BaseVault.sol#263) ) hs external calls inside = loop: mountPinest = ###t.miniamountConvert, asset.balance0f(address(this)) (contracts/BaseVault.sol#568) ) has external calls inside = loop: itrutegy_exp_l.invest(exprts/tasset.balance0f(address(this)).fortnats/BaseVault.sol#568) ) has external calls inside = loop: itrutegy_exp_l.invest(exprts/tasset.balance0f(address(this).fortnats/BaseVault.sol#567) ) has external calls inside = loop: itrutegy_exp_l.invest(exprts/tasset.balance0f(address(this).fortnats/BaseVault.sol#567) ) has external calls inside = loop: (success,result) = address(this).delegatecalldats(1)) (contracts/external/Nulticall.sol#12) ter=Concementation#calls=nnis#==-loop: teracts/polygon/L2Vault.sol#563) (contracts/BaseVault.sol#563) crticasfers@fund(amount) (contracts/sol#200,L2Vault.sol#562) ortformferre@fund(amount) (contracts/polygon/L2Vault.sol#552) ortformferre@fund(amount) (contracts/polygon/L2Vault.sol#552) org/L2Vault.sol#563); sismount) (contracts/polygon/L2Vault.sol#558) (L2Vault.sol#563); orgoon/L2Vault.sol#564-553); orgoon/L2Vault.sol#564-553); orgoon/L2Vault.sol#564-553);</pre>
BaseVau) BaseVau) BaseVau) BaseVau) BaseVau) BaseVau) Reference Reentrar Reentrar	cyclindreamlohume. degeneralith(init26) [contra (contrat(p))(of desegnery(p)(trasslowers) (contrat(p)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(contrats/laws)(contrats/laws) (contrats/laws)(co	<pre>tri(/objou/dmsrgmc/withdrawslQuue.sol#77-120) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawslQuuese(ptr,withdrawslQuuesee(ptr,withdrawslQuuese(ptr,with</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Reference Reentrar Reentrar	<pre>cptitdramalDuom.degramaBath(cint26) [contra [contractorphype] [contractorphy] [contractorphype] [contractorphy] [contractorphy] [contractorphy] [contractorphy] [contractorphy] [contractorphy] [contractorphysecu]. [trebalance[] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [trebalance] [contractorphysecu].aslb54-000 [contractorphysecu] [contractorphysecu].aslb54-000 [contractorphysecu] [contractorphysecu].aslb54-000 [contractorphysecu] [contractorphysecu].aslb54-0000 [contractorphysecu].aslb</pre>	<pre>tri/objoon/immergencyWithdramelQueue.sol#77-120) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdramelQueue(ptr,withdramelQue</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Multical Reference Reentrar Reentrar	opiinkaaa ]onee.degaaamatehinint260 [contra [contrati/phig/mideepochintaaa]oome.a it.reaovafartaggi[lassittegg] (contrati/hase it.reaovafartaggi] (contrati/hase/lune) it.reaolanee() [contrati/lassitul.asl640-000 it.reablanee() [contrati/lassitul/	<pre>tid/pippon/fmargencyWithdrawelQueue.sol#97-120) has external calls inside a loop: redexeedAssetAnount = vault.redexeMpImergencyWithdrawelQueue(ptr,withdrawelRec imp0-100) Vault.sol#264-271) has external calls inside a loop: meuntWithdrawe = strategy.divexf(type()(uint26).max) (contracts/BaseYault.sol#257) .) has external calls inside a loop: meuntWithdrawe = strategy.divexf(type()(uint26).max) (contracts/BaseYault.sol#257) .) has external calls inside a loop: meuntWithdrawe = strategy.divexf(type()(uint26).max) (contracts/BaseYault.sol#257) .) has external calls inside a loop: autoFitnery = state, s</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Multical Reference Reentrar Reentrar	<pre>cptithesalbus.deguasatch(init26) (contra (creased)raby(fasetaropy)(contract/base) (creased)raby(fasetaropy)(contract/base) (creased)raby(fasetaropy)(contract/base) (creased)raby(fasetaropy)(contract/base) (creased)raby(fasetaropy)(contract/base) (creased)raby(fasetaropy)(creased) (creased)raby(fasetaropy)(creased) (creased)raby(fasetaropy)(creased) (creased)raby(fasetaropy)(creased) (creased)raby(fasetaropy)(creased) (creased)raby(fasetaropy)(creased) (creased)(creased)(creased)(creased) (creased)(creased)(creased)(creased)(creased) (creased)(creased</pre>	<pre>tid/pippon/fmargencyWithdrawelQueue.tol#77-120) has external calls inside a loop: redexemdAssetAnount = vult.redexemdyEmergencyWithdrawelQueue(ptr,withdrawelRet ExeP-100) Vult.sol#246-271) has external calls inside a loop: mountWithdrawe = strategy.divex(type()(uint26).mas) (contracts/BaseVault.sol#257) .sol#247-463) has external calls inside a loop: mountWithdrawe = strategy.divex(type()(uint26).mas) (contracts/BaseVault.sol#257) .sol#247-463) has external calls inside a loop: mountWithdrawe = strategy.divex(type()(uint26).mas) (contracts/BaseVault.sol#263) .) has external calls inside a loop: aufortInters = #dth.sinfeasurtInterst = states.blancoff(sdtrastUb) (contracts/BaseVault.sol#503) .) has external calls inside a loop: aufortInterst = #dth.sinfeasurtInterst = #dth.sinfeasur</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Multical Reference Reentrar Reentrar	<pre>pditAdvanlphane.deguanaltch(init26)(contra (ontrati/phanp)/despectady(init26)(contrati/base) it.reave(init26)(init26)(contrati/base) it.reave(init26)(init26)(contrati/base) it.reave(init26)(init26)(contrati/base) it.reave(init26)(init26)(contrati/base)(init26)(init</pre>	<pre>tri/pippor/margancywithdrawalQueue.sol#97-120) has external calls inside a loop: redesedAesstAnount = vault.redeemByEmergencywithdrawalQueue(ptr,withdrawalRec ins6-169) Vault.sol#264-271) has external calls inside a loop: meunontWithdrawn = strategy.divest(type((usin280).max)(contracts/BaseYault.sol#257)) .) has external calls inside a loop: meunorDinest = ##th.min(meunorDinest, meunorDinest, meunorD</pre>
BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] BaseVau] Multical Reference Reentrar Reentrar	<pre>cpd:ideaalbuse.deguaaltch(init26) [contra f(remergerg)(desetfrage)(remergerg) [contract/barg][contract/barg][contract/barg] [contract/barg][contract/barg][contract/barg] [contract/barg][contract/barg][contract/barg] [contract/barg][contract/barg][contract/barg] [contract/barg][contract/barg][contract/barg] [contract/barg][contractb/barg][con</pre>	<pre>tri/noipun/fmargancywithdramalQueue.sol#97-120) has external calls inside a loop: redeemedAesstAmount = vault.redeemByEmergencywithdramalQueue(ptr,mithdramalRec 1648-160) Vunlt-sol#264-271) has external calls inside a loop: menontWithdram = strategy.divest(type(((un126).max)(centracts/BaseYault.sol#257)) .) has external calls inside a loop: amountWithdram = strategy.divest(type(((un126).max)(centracts/BaseYault.sol#257)) .) has external calls inside a loop: amountWithdram = strategy.divest(type(((un126).max)(centracts/BaseYault.sol#257)) .) has external calls inside a loop: amountWithdram = strategy.divest(type(((un126).max)(centracts/BaseYault.sol#257)) .) has external calls inside a loop: attrategy.divest(centratts/BaseYault.sol#257) .) for formation / for trats/BaseYault.sol#250 .) for formation / for trats/BaseYault.sol#250 .) for formation / for trats/BaseYault.sol#250 .) for trats/BaseYault.sol#250 .) for trats/BaseYault.sol#255) .//Ault.sol#250 .//Ault.sol#250 .//Ault.sol#250 .//Ault.sol#250 .//Ault.sol#250 </pre>
BaseYau) BaseYau) BaseYau) BaseYau) BaseYau) BaseYau) BaseYau) BaseYau) Reentrar Reentrar Reentrar	opiinkamaalonaa.dagaamalathikinit260 [contra [contrati/bupi/dimespiceybi/bitrasellowup.at 1:resortsi/bupi/dimespiceybi/bitrasellowup.at 1:resortsi/bitratej]) [contrati/base/bit 1:resolance] [contrati/Base/ull.sol464-040 1:resolance] [contrati/Dase/ull.sol464-040 1:resolance] [contrati/Dase/ull.sol464-040] [contrati/Dase/ull. 1:resolance] [contrati/Dase/ull.sol464-040] [contrati/Dase/ull. 1:resolance] [contrati/Dase/ull.sol464-040] [contrati/Dase/ull. 1:resolance] [contrati/Dase/ull.sol464-040] [contrati/Dase/ull.sol4644-040] [contrati/Dase/ull.sol4644-040] [contrati/Dase/ull.sol4644-040] [contrati/Dase/ull.sol4644-040] [contrati/Dase/ull.sol4644-040] [contrati/Dase/ull.sol4644-040] [contr	<pre>tri/noipun/fmargancywithdramalQueue.sol#77-120) has external calls inside a loop: redeemdAssetAnount = vult.redeemByEmergencywithdramalQueue(ptr,mithdramalRet FMS-100) Vult.sol#264-271) has external calls inside a loop: mountwithdrama = strategy.divest(type((unit26).max)(contracts/BaseVault.sol#257) .sol#407-463) has external calls inside a loop: mountwithdrama = strategy.divest(type((unit26).max)(contracts/BaseVault.sol#257) ) has external calls inside a loop: mountWithdrama = strategy.divest(type((unit26).max)(contracts/BaseVault.sol#263)) ) has external calls inside a loop: mountWithdrama = strategy.divest(type()(unit26).max)(contracts/BaseVault.sol#263)) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#263) ) contracts/BaseVault.sol#264) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#264) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#265) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#264) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#265) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#265) ) has external calls inside = loop: strategy.divest(contracts/BaseVault.sol#265) ) has external calls inside = loop: strategy.di</pre>
BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) Reference Reentrar Reentrar Reentrar Reference Reference Reentrar	<pre>cpd:ideaalbuce.deguaaltch(in1250) [contra for more of degraphy of the selection of the resolution of degraphy of the selection of the resolution of degraphy of the selection of the resolution of the selection of the selection the selection of the selection of the selection the selection of the selection of the selection the selection of the selection of the selection of the selection of the selection of the selection of the selection the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection of the selection the selection of the selection of the selection of the selection of the selection of the selection of the selection the selection of the selection of the selection of the selection of the selection of the selection of the selection the selection of the selection of the selection of the selection the selection of the selection of the selection of the selection the selection of the selection of the</pre>	<pre>tid/pippon/fmargencyWithdramelQueue.tol#77-120) has external calls inside a loop: redereedAesetArount = vult.redereEdAesetArount = vult.rederEdAesetArount = vult.rederEdAesetArou</pre>
BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu Reentrar Reentrar Reentrar Reentrar Reentrar Reentrar	<pre>cpiintary_piinta</pre>	<pre>trip/nb/marganc/withdrawelQueue.sol#77-120) has external calls inside a loop: redexedAssetAnount = vult.redexedAssetAnount = vult.redexedAssetA</pre>
BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu Reentrar Reentrar Reentrar Reentrar Reentrar	<pre>cpiinkaaalbana.dagaamatathiciint260 [contra [contration][contration][contration] [contration][contration][contration] [contration][contration][contration] [contration][contration][contration][contration] [contration][</pre>	<pre>trip/nopun/fmargencyWithdramelQueue.sol#77-120) has external calls inside a loop: rederedAssetArount = vult.rederedAssetArount = vult.redereAss</pre>
BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) BaseYuu) Reference Reentrar Reentrar Reentrar Reentrar Reference Reference Reentrar	<pre>cpiinkamalbume.degumentshich(in1260) [contra [contration](might despiped)(threase]courses 1; removed)reign(despiped)(threase]courses 1; removed)reign(despiped)(threase]courses 1; removed)reign(despiped)(threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; removed)(threase](threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; removed)(threase]courses 1; threase]courses 1; threase 1; threase]courses 1;</pre>	<pre>trip/nb/par/margancywithdrawelQueue.sl#77-120) has external calls inside a loop: redeemdAssetAnount = vult.redeemByEmergencyWithdrawelQueue(ptr,withdrawelRet Fuld-169) Vult.suf264-721) has external calls inside a loop: mountWithdrawn = xrstmy, divex(type()(u(n126),max)(contracts/BaseVault.suf257) ) has external calls inside a loop: mountVithdrawn = xrstmy, divex(type()(u(n126),max)(contracts/BaseVault.suf257) ) has external calls inside a loop: mountVithdrawn = xrstmy, divex(type()(u(n126),max)(contracts/BaseVault.suf257) ) has external calls inside a loop: intraty/gaveTuelLeckedWult.suf250) ) has external calls inter suf250) ) has external calls inter suf</pre>
BaseVua) BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala BaseVala Reentrar Reentrar Reentrar Reentrar	pyithWaselDames.degrammatch(min260) [contrat/ pointrat/pubged/despecybed/hitselDawes. 1; resortSirtigy/[lasdirtigy] (contrati/hese 1; resortSirtigy/[lasdirtigy] (contrati/hese 1; resortSirtigy/[lasdirtigy]) (contrati/hese 1; resortSirtigy]) (contrati/hese 1; res	<pre>trip/nb/marganc/withdrawelQueue.ub/#77-120) has external calls inside a loop: redeemdAssetAnount = vult.redeemByEmergencyWithdrawelQueue(ptr,mithdrawelRec Fuld-100) Vult.solf260-71) has external calls inside a loop: meunotWithdrawe = stratey,disex(type)((uin126),max)(contracts/BaseVault.solf257) ) has external calls inside a loop: meunotYmete = with.min(meunotUnivet, samet.balance/fulde() (contracts/BaseVault.solf257) ) has external calls inside a loop: meunotYmete = with.min(meunotUnivet, samet.balance/fulde() (contracts/BaseVault.solf257) ) has external calls inside a loop: meunotYmete = with.min(meunotUnivet, samet.balance/fulde() (contracts/BaseVault.solf257) ) has external calls inside a loop: meunotYmete = with.min(meunotUnivet, samet.balance/fulde() (contracts/BaseVault.solf257) ) has external calls inside a loop: meunotYmete = with.min(meunotUnivet, samet.balance/fulde() (contracts/BaseVault.solf257) ) has external calls inside a loop: meunotYmete() = with a stratege/fulde() (contracts/BaseVault.solf257) (meunotUnivet)/sameters/fulde() (contracts/BaseVault.solf257) ) has external calls inside = hos: (wacces.result) = widfes(this).elegatesall(data(1)) (contracts/sternal/Multicall.solf17) terd-fulde()/vault.solf267-538): terd-fulde()/vault.solf267-538): terd/fulde()/vault.solf267) sters/fulde()/vault.solf263) (contracts/polyon/L2Vault.solf263) (contracts/polyon/L2Vault.solf264-553): elygon/(L2Vault.solf264-553):</pre>
Bas Vuo Bas Vuo Bas Vao Bas Vao Bas Vao Bas Vao Bas Vuo Bas Vu	<pre>cpditimesalpumes degrammatch(init26) (contrat/ pointar(p)(m)(freeproprint)(freeproprint) in removediratopy(lassifratopy) (contratt/her in removediratopy(lassifratop)) (contratt/her intreat).contratt/markut.sid54-000 intreat).contratt/markut.sid54-000 intreat).contratt/markut.sid54-000 intreat).contratt/markut.sid54-000 intreat).contratt/markut.sid54-000 intreat).contratt/markut.sid54-000 intreat].contratts/polyno/ intreat].contratts/polyno/ intreat].sid54-000 intreat].contratts/polyno/ intreat].sid54-000 intreat].sid</pre>	<pre>rty/spec/fmegenc/withdramellouse.sl#97-138) has external calls inide a loop: redeemeddatetAmount = vault.redeemByEmegenc/withdramellouse(ptr,</pre>
Bas Vuo Bas Vuo Bas Vao Bas Vao Bas Vao Bas Vao Bas Vuo Bas Vu	pylithamas Damas.deparamilth(init26) [contra [contrat/ph/pp/1/sepsoproj/thirase]Damas bit removeStrategy[lasStrategy] (contratt/Basel litrasetStrategy]] (contratts/Basel litrasetStrategy]] (contratt/Basel litrasetStrategy]] (contratt/Palagon/24000) - contrast/Basel litrasetStrategy]] (contratt/Palagon/24000) - contrasterStrategy] (contrast/Basel litrasetStrategy]) (contratt/Palagon/24000) - contrasterStrategy] (contrast/Basel litrasetStrategy]) (contrast/Palagon/24000) - contrasterStrategy] (contrasterStrategy]) (contrast/Palagon/24000) - contrasterStrategy] (contrasterStrategy]) (contrast/Palagon/24000) - contrasterStrategy] (contrasterStrategy]) (contrast/Palagon) (contrasterStrategy]) (contrasterStrategy]) (contrasterStrategy] (contrasterStrategy]) (contrasterStrategy]) (c	<pre>rty/spec/fmegenc/withdramellouse.sl#97-138) has external calls inide a loop: redeemeddatetAmount = vault.redeemByEmegenc/withdramellouse(ptr,</pre>

Ex	RequestFont[innont] (contracts/noligon/L2Wult.solB68) yin L2Wult.transferTol[uint266) (contracts/polygon/L2Wult.solB640-653): ternal calls:
	bridgsEcrow.l2Withdraw(asount) (contracts/polygon/L2Vault.sol8543) want emitted after the call(s): TranferToLitaaount) (contracts/polygon/L2Vault.sol8544)
Reentrancy Ex	/h/dsWull.appoint/hostriegy.dsustriegy.unit260 (contract//dsevull.sol#2/2-30/): articles_interview.dsevull.appoint/sol#270 (contract//dsevull.sol#27) (contract//dsevull.sol#27)
Reentrancy	vent emitted after the coll(s): StrategyDeposit[strategy,tokenAnnount] (contracts/BaseVault.sol#338) / in EmergenerWithdramalDueue.dequeue() (contracts/polygan/EmergencyWithdrawalDueue.sol#79-94):
	<pre>ternal colls: redeemedAssetAmount = vault.redeemByEmergencyWithdrawslQueue(headPtr,withdrawslRequest.shares,withdrawslRequest.receiver,withdrawslRequest.owner) (contracts/polygon/EmergencyWithdrawslQueue.sol#85-87 ent emitted after the coll(s):</pre>
- Reentrancy Ex	EmergencyWithdrama]QueueDequeue(headPtr,withdrama]Request.comer,withdrama]Request.shares) (contracts/polygon/EmergencyWithdrama]Queue.sol#89-91) / in EmergencyWithdrama]Queue.dequeueBatch(uint256) (contracts/polygon/EmergencyWithdrawa]Queue.sol#87-120): ternal calls:
	redeemedAssetAmount = vault.redeemByEmergencyWithdrawalQueue(ptr,withdrawalRequest.shares,withdrawalRequest.receiver,withdrawalRequest.comer) (contracts/polygon/EmergencyWithdrawalQueue.sol#106-108) rent emitted after the call(s):
	EmergenykithdrawalQueueOeguuu(headdtr.w.sthdrawalRequest.emer.w.thdrawalRequest.emergeneykithdrawalQueue.sol#18-112) in L2Wernbladbuter.reseiv¥umidikfytes) (ontracts/polygon/2Wormhol#Roter.sol#56-56): ternal =alls: vull.bridgeEscrw().l2ClearFund(amount) (contracts/polygon/2Wormhol#Roter.sol#54)
	vent emitted after the call(s): TransferFondL(manurt) (contracts/polygon/L2WormholeRouter.sol#55) in BasVault-withdrawFondErategy(BaseStrategy.uint256) (contracts/BaseVault.sol#362-376):
	<pre>cternal calls: appund/tithurawn = strategy.divest(tokenAmpunt) (contracts/BaseVault.sol#866)</pre>
	vent emitted after the coll(s): Strategykithorewl(strategy, amountWithdrawn) (contracts/SaseYault.sol#374) : https://github.com/crytic/slither/wiki/Datector-Documentation#reentrancy-vulnerabilities-3
Da	harvest(8aseStrategy[]) (contracts/8aseVault.sol#407-462) uses timestamp for comparisons ngerous comparisons: remutrachom istical(hinck.timestame.az lastHarvest + lockToterval PROETT UNIOCKING) (contracts/BaseVault.sol#400)
Da	require(bol,string)(block.timestamp>= lastWarvest + lockInterval,PROFT_UNLORKIND) (contracts/BaseVault.sol#409) lockedPort[i](contracts/BaseVault.sol#468-473) uses timestamp for comparisons block.timestamp>= lastWarvest + lockInterval (contracts/BaseVault.sol#469)
EmergencyW	vithdrawallueu.deuuue() (contracts/polygon/EmergencyWithdrawalQueue.sol#79-94) uses timestamp for comparisons nomerous comparisons
Da	redeenddasstAnount > 0 (contracts/polygon/EmergencyWithdrawalDueue.sol#88) ssessFeas() (contracts/polygon/LZYwult.sol#62-73) uss timestamp for comparisons ngrous comparisons:
L2Vault.re Da	numBharssTaWint == 0 (contracts/polygon/LYWult.sol#80) demByBergencywihdramalDuwulnic1250,uit252,defres,defres,defres,defres,defres,defres,defres,defres,defres,defres, ngerous comparisons: BalanceOffommer ( e marse (contracts/polygon/LYWult.sol#218)
L2Vault.re Da	odeemuuntzob,aodress,aodress) (contracts/polygon/Lzvauit.sol#239-2/4) uses timestamp for comparisons ingetous comparisons:
- L2Vault.wi Da	requirchool.string(idhars - emergencyWithdramalQueue.debtToDuner(owner) << balanceOf(owner),Not enough share available in owners balance) (contracts/polygon/L2Vault.sol#240-243) ithdraw(uint26, address, address) (contracts/polygon/L2Vault.sol#277-317) uses timestamp for comparisons macrous comparisons:
L2Vaultc	require(bloc),strip(HSA)stars - sergencyb(Hofrae)Leave,deUTdOmer(omer) <= balanced(former), Not entyp host require(blocy), strip(HSA)stars - sellable) (contracts/polygon/LZVeult.sol#283-286) contracts - sergencyb(HSA)strip(HSA
L2Vault. c	totalBhars == 0 (contracts/oolygon/L2Vault.sol#344) mowretChasster (murd26,L2Vault.monding) (contracts/polygon/L2Vault.sol#341-373) uses timestamp for comparisons totalBhars == 0 (contracts/polygon/L2Vault.sol#343)
L2Vault.lo	bckedTVL() (contracts/polygon/L2Vault.sol#468-475) uses timestamp for comparisons
L2Vault.de	nngereux comparisons: Ibok-timestams isatVUUpdate + lockInterval (contracts/polygon/LZVult.sol#680) Ibok-timestams (contracts/polygon/LZVult.sol#680-564) uses timestamp for comparisons Ingereux scomestions:
	nngercus comparisons: totalSuppi(): 0 @ (cntracts/polygon/LZVault.sol#552) : https://github.com/crytic/slither/wiki/Detector-Documentation#Dlock-timestamp
	multicallbyts()) (contracts/external/Multicall.sol89-27) uses assembly ]MLIME ASM (contracts/external/Multicall.sol89-21) .htps://glimb.on/crytics/inter/aki/Detect-obcumentation#assembly-usage
EmergencyW	withdrawalQueue.degueueBatch(uint256) (contracts/polygon/EmergencyWithdrawalQueue.sol#97-120) has costly operations inside a loop:
BaseVault. BaseVault.	dolste guwun[str] (contracts/polygon/Emergencywiihdrawallouwe,sol/H33) .removeStrategy(BaseStrategy) (contracts/BaseYault.sol#244-271) has costly operations inside a loop: totalgbs = stratinfo.tvlBps (contracts/BaseYault.sol#244-271) has costly operations inside a loop: total3trategy(BaseStrategy) (contracts/BaseYault.sol#244-271) has costly operations inside a loop: total3trategy(BaseYault.sol#244-271) has costly operations inside a loop: total3trategy(BaseY
BaseVault.	removeStrategy(BaseStrategy) (contracts/BaseVault.sol#240-271) has costly operations inside a loop:
BaseVault.  BaseVault.	maxicskedProfit ++ sldB31 - amountWithdram (contrasts/BasWault.sl2#27) updatstrzegybulcscinne(BasKattagef),unit25(1)(contrasts/BasWault.sl2#278-277) has costly operations inside a loop: trashp= moltDpu (contrasts/BasWault.sl2#23) trashp= northorizats/BasWault.sl2#23) trashp= northorizatBas(contrasts/BasWault.sl2#29) trashp= northorizatBas(contrasts/BasWault.sl2#29)
Reference:	: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop
L2Vaultm	,_assesfees() (contracts/BaaVault.sol#122-129) is never used and should be removed segData() (contracts/polygon/L2Vault.sol#122-129) is never used and should be removed https://github.on/crytic/silter/wiki/Detector-Documentation/dead-code
Pragma ver Pragma ver	rsion®-8.8.13 (contracts/AffineGovernable.sol#2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/8.8.7 rsion®-8.13 (contracts/BaseStrategy.sol#2) necessitates a version too recent to be trusted. Consider deploying mith 8.6.12/0.7.6/8.8.7 rsion®-8.13 (contracts/BaseSurit.sol#2) necessitates a version too recent to be trusted. Consider deploying mith 8.6.12/0.7.6/8.8.7
Pragma ver Pragma ver Pragma ver	rsion®.4.31 (contracts/MaevAult.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rsion®.8.13 (contracts/StidgeScrew.ol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rsion®.8.18 (contracts/Constants.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma ver Pragma ver Pragma ver	exion®.4.31 (contracts/NormholRouter.solf2) necessitates a version too recent to be truxted. Consider deploying with 8.6.12/0.7.6/0.8.7 exion®.8.13 (contracts/stermal/Multicall.solf4) necessitates a version too recent to be truxted. Consider deploying with 8.6.12/0.7.6/0.8.7 exion®.8.13 (contracts/interfaces/IEGKAd2.solf2) necessitates a version too recent to be truxted. Consider deploying with 6.6.12/0.7.6/0.8.7
Pragma ver Pragma ver Pragma ver	rsion9.8.13 (contracts/interfaces/IRootChainManagor.sol2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.8.7 rsion9.8.13 (contracts/interfaces/IVault.sol2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.8.7 rsion9.8.13 (contracts/interfaces/IVault.sol2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/8.7.6/8.8.7
Pragma ver Pragma ver Pragma ver	rsion® 8.13 [contracts/linerfaces/[Wull.sol#2] necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/0.8.7 rsion® 8.13 [contracts/linerfaces/[Wull.sol#2] necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rsion® 8.13 [contracts/polygon/Detailed.sol#2] necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rsion® 8.13 [contracts/polygon/Detailed.sol#2] necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rsion® 8.13 [contracts/polygon/Detailed.sol#2] necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 rsion® 8.13 [contracts/polygon/Detailed.sol#2] necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
solc-0.8.1	rsion 9.8.18 [contracts/polypoin/l/20ormholeAbuler.solf2] messing to share to share to be rusted. Consider deploying with 8.6.12/0.7.6/0.8.7 16 is not recommended for deployment https://dithuo.on/crytics/ithre/wiki/Detector-Documentation#incorrect-versions-of-solidity
	<pre>:ncip://girub.com/cfylip/silner/mark/Detector-vocumentium.morfedc=versims=or=silnity call im Niticall.multicall(byte()) (contract/Multicall.sol=27): (uccess.result.multicall(byte(i)) (contract/determan/Multicall.sol=27)</pre>
	(Success,rsuit) = dorr5sithis).adidgsteall(satl)) (contracts/sithal/Multislls01#12/) https://githus.on/rytio/sithus/wiki/Butesto-Doumentiation/Bun-Fuel-abl contracts/polygon/L2Vault.sol#29-589) should inherit from 1L2Vault (contracts/interfaces/lVault.sol#8-10)
Reference:	omtract/fpsigdp/Lv/ault/solf24-ba9/ishou/a inmerit trom L2#ault (contracts/inferres/i#ault.solf29-b9) https://gltub.com/cytic/silfuter/wiki/Detect-Documentialomising-inmeritinne expression *receiver (contracts/polygon/L2#ault.solf41A)* inL2#ault (contracts/polygon/L2#ault.solf29-569)
Redundant	*#ression *receiver (contracts/polygon/lZVault.sol#A14)* intZVault (contracts/polygon/lZVault.sol#29-589) #xression *receiver (contracts/polygon/lZVault.sol#A29* intZVault (contracts/polygon/lZVault.sol#29-589) : https://github.com/crytic/slither/wiki/Datestor-Documentation#redundant-statements
Variable B Variable C	BaseVault.swapHithdrawalQueueIndexes(uint256,uint256).newStrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.swapHithdrawalQueueIndexes(uint256,uint256).newStrategy2 (contracts/BaseVault.st_PUND_TRANSFER_BEPORT (contracts/Constants.col#2)) is too similar to Constants.12_FUND_TRANSFER_BEPORT (contracts/Constants.col#2) +
BaseStrate	: https://github.com/rytic/slither/wiki/Betector-DocumentationHvariable-names-are-too-similar agy (contracts/BaseStrategy.sol#9-48) does not implement functions:
	BasBtratey,Just(int26) (contract/BasBtratey.s0125) BasBtratey.Just(int26) (contract/BasBtratey.s0126) BasBtratey.Juset(int25) (contract/BasBtratey.s0126) BasBtratey.Juset(int25) (contract/BasBtratey.s0126)
	BaseStratey.totalLockedValue() (contracts/BaseStratey.sol#41) : https://github.com/crytic/slither/wiki/Detector-Documentation#unimplemented-functions
Reference:	cow.vaulMance (contracts/BridgeEscrow.solM9) should be constant : https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
	nuld be declared externis: BaseMault.asset() (contracts/BaseMault.sol#33-35) 12Mault.asset() (contracts/polygon/LZWault.sol#149-151)
multicall( 	(bytes[]) should be declared external: Multicall.multicall(bytes[]) (contracts/external/Multicall.sol#9-27) (Zwalt) should be declared external:
totalDebt(	EmergencyWithdrawalDouww.JinVault[[vault] [contractspolygen/EmergencyWithdrawalDouww.sel#46-57] 1 shalls de defande arternal: 1 shalls de defande arternal:
	e(address,ERC29,address,BridgeEcrow,EwergencyWithdrawalQueue,address,uint266,uint256(u)) hould be declared external: L'Avault.intilizie(address,ERC29,address,HidgeEcrow,EergencyWithdress,uint26,uint256,uint256(u)) (contracts/polygon/L2Vault.sol#83-110)
convertToA:	harse(unit26a) ahould be declared external: 1/2/unit.convertBoharse(unit26a) (contracts/polygon/L2Yult.sol#336-337) seats(unit25b) ahould be declared external: 1/2/unit amounter/factor
	L2Vault.convertToAssets(init266) (contracts/polygon/L2Vault.sol#356-358) Henc(init266) havoul de hedclared external: L2Vault.previewRedeen(uint256) (contracts/polygon/L2Vault.sol#391-393)
	(address) should be declared external: [Vault.maxDepsi(iddress) (contract/sployen/LZWalt.sol#43-416)
maxMint(ad	idress) should be declared external:
maxMint(ad -   maxRedeem(; -	ddress) hould be declared external: 2/Wault.madWint (ddress) (contracts/polygon/L2Vault.sol#439-422) address) should be declared external: 2/Wault.macRedensidadress) (contracts/polygon/L2Vault.sol#436-427)
maxMint(ad -   maxRedeem(; -   maxWithdra	idress) hohuld be declared external: L2Vault.maxMint(address) (contracts/polygon/L2Vault.scl#419-422) address) should be declared external:

# src/polygon/L2WormholeRouter.sol

Referenc	<pre>l.multicall(bytes()) (contracts/external/Multicall.sol#9-27) has delegatecall inside a loop in a payable function: (success,result) = address(this).delegatecall(data[i]) (contracts/external/Multicall.sol#12 - https://github.com/crytic/slither/wiki/Detector-Documentation/Apayable-functions-using-delegatecall-inside-a-loop</pre>
	tegy.wult (contracts/BaseStrategy.sol#13) is never initialized. It is used in:
	tegy.vault (contracts/BaseStrategy.sol#13) is never initialized. It is used in: - BaseStrategy.seep(ERC20) (contracts/BaseStrategy.sol#20-47) tegy.seet(Contracts/BaseStrategy.sol#21) is never initialized. It is used in: - BaseStrategy.seexep(ERC20) (contracts/BaseStrategy.sol#30-47) = https://github.contracts/BaseStrategy.sol#30-47) = https://github.contracts/BaseStrategy.sol#30-47)
L2Vault.	_sessifies() (contract/polypoy/LYWu)L.sol#62-73) exptores a multiplication on the result of a division: -feedbas (duration # managementies) /SECS_PK.VAR (contract/polypoy/LYWult.sol#64) -numSharesTMAInt = (feesbage = tot3SegDy()) / MXS_BS (contract#/polypoy/LYWult.sol#64) = https://github.contractif.divisither/skil/Detectro-Documentaliand/side=Hoferco-multiply
L2Vault.	<pre>assesses() (cortract/polygon/LZYwalt.sol#62-73) uses a dangerous strict equality: - undBharafoldint = 0 (contract/polygon/LZYwalt.sol#63) convertOdsset(uint26,LZYwalt.Rounding) (contract(polygon/LZYwalt.sol#361-373) uses a dangerous strict equality: - totalibharss = 0 (contract/polygon/LZYwalt.sol#636) - totalibharss == 0 (contract/polygon/LZYwalt.sol#646-353) uses a dangerous strict equality: - totalibharss == 0 (contract/polygon/LZYwalt.sol#646-353) - totalibharss == 0 (contract/golygon/LZYwalt.sol#646-3546-353) - asountOrivest == 0 (contract/golygon/LZYwalt.sol#646-3546-353) - asountOrivest == 0 (contract/golygon/LZYwalt.sol#646-3547-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-368) uses a dangerous strict equality: - doltabarss == 0 (contract/golygon/LZYwalt.sol#6477-3677-36777-367777777777777777777777</pre>
L2Vault.	<pre>cotlBhares == 0 (contracts/polygon/tZvult.sol836) convertOshares(lutt85,tZvult,lsuuding) (contracts/polygon/tZvult.sol8360-353) uses a dangerous strict equality;</pre>
BaseVau]	<ul> <li>totilbases == @ [contract/paper/1Kuoli.sol944]</li> <li>totilbases == @ [contract/paper/1Kuoli.sol944-9b] uses a dangerous strict equality:</li> </ul>
L2Vault.	receivPY(uinit86,bool) (contracts/polypom/L2Vault.solPA77-500) uses a dangerous strict equality: - data = 0 (contracts/polypom/L2Vault.solPB0)
Referenc	e: https://github.com/cryiic/slither/wiki/betector-bocumentation#dangerous-strict-equalities cy in EmergencyWithdrawalQueue.dequeue() (contracts/polygon/EmergencyWithdrawalQueue.sol#79-94):
	External calls:
Reentrar	- redeemeddasetAmount = vull:rdeemByRergencyWithdrawalDeuw(headPtr,withdrawalRequest.shares,withdrawalRequest.cosiver,withdrawalRequest.cwner) (contracts/polygon/EmergencyWithdrawalDeuwe.sol#85-87) state variables writem after the call(s): - headPtr == 1 (contracts/polygon/EmergencyWithdrawalDeuwe.sol#87-802);
Referenc	- balanchisMervet = strategy.totall.oksdWillow() (contracts/BaseYault.sol#432) State variables written after the call(s): - strategies[strategy].solance = balanceThisMervet (contracts/BaseYault.sol#435) = https://github.conforty161/Bithervist1Detecto-DocumentalianGasentancey-uninarbilities-1
BaseVaul L2Vault.	torganitéMithdrawalQueue().offset (contracts/BeseVault.sol#229) is a local variable never initialized c.harzest(BaseStrategr[).totalProfitAcrued (contracts/BeseVault.sol#248) is a local variable never initialized compotéMainare().invest (contracts/polygn/Vault.sol#260) is a local variable never initialized c.htgs://github.contcrytics/Intervisi/Detecto-Documentation/Initialized/local-variables
Referenc	e: https://github.com/cryti/slither/wiki/Detector-Documentation#uninitialized-local-variables
BaseVaul L2Wormho	t.rebalnos() (contracts/BasYuult.sp1840-500) ipposes ratum value by strategy.divest(cur5trategyTL.) (contracts/BasYuult.sp1840-500) ipposes ratum value by strategy.divest(cur5trategyTL.) (contracts/BasYuult.sp1840-500) ipposes ratum value by strategy.divest(cur5trategyTL.) (contracts/BasYuult.sp1840-500) ipposes ratum value by strategy.divest(cur5ts/BasYuult.sp1840-500) ipposes ratum value by strategy.divest(cur5ts) (contracts/BasYuult.sp1840-500) ipposes ratum value by strategy.divest(cur5ts) ipposes ratum value by strategy.dippose ratum value by strategy ratum value by strategy ra
	t.basinitialize(address,ERC20,address,BridgeEscrew) (contracts/BaseVault.sol#37-54) should emit an event for: - governance = governance (contracts/BaseVault.sol#42) - btrac/(doithe.ord/cruid.al/thar/bii/IDmatrationedmision_events_rocass_control
L2Vault.	e: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-access-control setManagementFee(uint256) (contracts/polygon/L2Vault.sol#56-56) should emit an event for:
	- managementfee = feeBps (contracts/polygon/L2Vault.sol#55) setWithtramalFee(uint26) (contracts/polygon/L2Vault.sol#56) = withdramalFee = feeBps (contracts/polygon/L2Vault.sol#55)
	- withdrawalfee = *emBp (contracts/solgom/L2Wult.sol#59) mithiliz(address,ERC2)address,BridgeScrow,EergencyWithdrawalQueue,address,uint256,uint256(2]) (contracts/polygon/L2Wult.sol#83-110) should emit an event for: - 1Ratio =
	- 12Ratio = _12Ratio (contracts/polygon/L2Wault.sol#188) - windrawalFee = fees[0] (contracts/polygon/L2Wault.sol#188)
	net operative (-1-20)
	- 139atio = _139atio (contracts/psly@n/129ult.sol3455) regiveTv(LingtsK),bob)((contracts/psly@n/129ult.sol347559),bobuld emit an event for:
Referenc	- 128atio (contract/polygon/l2Vault.sol#188) = intramamice = fems(8) (contract/polygon/l2Vault.sol#188) setLaverSation(cint256.uint266) (contract/polygon/l2Vault.sol#469-652) should smit an event for: - l3Ratio = l3Ratio (contract/polygon/l2Vault.sol#465) = l3Ratio = l3Ratio = largen/l2Vault.sol#465) = l3Ratio = l3Ratio = largen/l2Vault.sol#465) = l3Ratio = l3Ratio = largen/l2Vault.sol#465 = l3Ratio = l3Ratio = largen/l2Vault.sol#465 = l3Ratio = l3Ratio = largen/l2Vault.sol#465 = largen/l2Vault.s
	crow.constructor(sddress).comer (contracts/BridgeEscrow.sol#28) lacks a zero-check on ;
	- emmer = _ommer (contracts/BridgeEscrow.sol#29) crow.initialize[address,]RootChsimAmager]ault (contable address) lacks a zero-check on : - wailt = _wullt (contracts/BridgeEscrow.sol#35)
	- wult = _wult (contacts/#idgeEcrow.sold35) - morbholdoutsr Bussyault_wult / wont/ worbholRouter() (contracts/BridgeEcrow.sol#36) / assantitalize(address, ERC30, address, EridgeEscrow). governance (contracts/BaveYault.sol#37) lacks a zero-check on : 
	<ul> <li>povernance =_governance (contracts/BaseVault.sol#42)</li> <li>t.basaTititalize(address, 5K28, dddress, 5K28, dddress, gridgeEscrew) _mornholeNouter (contracts/BaseVault.sol#37) lacks a zero-check on :         worsholeNouter (_wornholeNouter (contracts/BaseVault.sol#44)</li> </ul>
L2Wormho	leRouter.initialize(IWormhole,L2Vault,address.uint16), otherLaverRouter (contracts/polygon/L2WormholeRouter.sol#18) lacks a zero-check on :
	- otherLayerBourder = otherLayerBourder (contracts/polyGon/L3MesmboleRouter.col275) e: https://github.com/crytic/slither/wiki/Detector-DocumentationRmissing-zero-address-validation 
BaseVau]	yWithdrawalQueux.dequeuBBsthluint256) (contracts/polypon/EmergencyWithdrawalQueue.sol#97-128) has external calls inside a loop: redeemedAssetAmount = vault.redeemByEmergencyWithdrawalQueue(ptr,withdrawalRe (contracts/polypon/EmergencyWithdrawalQueue.sol#186-188) r.remov&strategy(Base&strategy)(contracts/BaseWault.sol#260-271) has external calls inside a loop: amountWithdrawal redeemByEmergencyWithdrawalQueue(ptr,withdrawalRe r.remov&strategy(Base&strategy)(contracts/BaseWault.sol#260-271) has external calls inside a loop: amountWithdrawalRet(taug)(contracts/BaseWault.sol#267)
BaseVaul BaseVaul	t.harves(f8seStrategy()) (contracts/BsseVault.sol#640-662) has external calls inside a loop: balanceThisHarvest = strategy.totallockedValue() (contracts/BaseVault.sol#632) t.rablance() (contracts/BaseVault.sol#640-640) has external calls inside a loop: balanceThisHarvest = strategy.totallockedValue() (contracts/BaseVault.sol#632)
BaseVau] BaseVau] BaseVau]	t.rebalancs() (contract/BaseYuult.sol854-590) has external calls inside a loop: strategy_scope_l.invest(mountFolnvest) (contracts/BaseYuult.sol854-590) has external calls inside a loop: currEntategyTVL = strategy_stol2(contracts/BaseYuult.sol8565) t.rebalancs() (contracts/BaseYuult.sol854-590) has external calls inside a loop: currEntategyTVL = strategyTVL = idealStrategyTVL (contracts/BaseYuult.sol8565) t.rebalancs() (contracts/BaseYuult.sol854-590) has external calls inside a loop: strategy.divest(currStrategyTVL = idealStrategyTVL) (contracts/BaseYuult.sol8565)
Multical	<pre>L.multiall(bytes()) (contract/external/Multiall.sol#-27) has external calls inside a loop: (success, result) = address(this).delagatecall(data[i]) (contract/external/Multicall.sol#12) e: https://github.com/crytic/slither/wiki/Detector-Documentation/fcalls-inside-a-loop</pre>
	cy in L2VaultL1L2Rebalance(bool,uint256) (contracts/polygon/L2Vault.sol#527-538): External calls:
	<ul> <li>liguidate(amount) (contracts/polygon/L2Vault.sol#531)</li> </ul>
	- amountWithdram = strategy.dives(fchendmount) (contracts/BaseYault.sol#364) - transferTolliamunToSomd( contracts/oplogno/LZVult.sol#363) - pridgeEarow.jZVithdrawiamunt) (contracts/oplogno/LZVult.sol#352) - LZVerMoleAbudter(wentScheldbuter: record:Transferzedput(amount) (contracts/oplogno/LZVult.sol#352)
	<ul> <li>200sth0l#Douts/issubla@outs/.sportTransferredFund(amount) (contracts/polygon/L2Vault.sol#552)</li> <li>State variables written after the call(s): transferTol(lamountToBand) (contracts/polygon/L2Vault.sol#533)</li> </ul>
Reentran	transereiGitamountiosamoj (contractis/poijgon/L/valit.sol#sa)) animuleriGit = false (contracts/poiygon/L/Valit.sol#S6)> cy in L2Valit_divestFomLluint256) (contracts/poiygon/L2Valit.sol#S57-561): External calls:
	- L2WormholeRouter(wormholeRouter).requestFunds(amount) (contracts/polygon/L2Vault.sol#558) State variables written after the call(s):
	- canRequestFronL1 = false (contracts/polygon/L2Vault.sol#559) cy in L2Vault_transferColl(uint256) (contracts/polygon/L2Vault.sol#548-553): External colls:
	- bridgeEscrom.1RWithdraw(amount) (contracts/polygon/LZVault.sol#563) State variables written stret the call(s):
	- LiTotilockeXVilu = * amount (contracts/polygon/L2Vult.so18549) - contransferioli = folse (contracts/polygon/L2Vult.so18548)
	cy in BaseNuult.removeStrategy(BaseStrategy) (contrats/BaseVult.sol#240-271): External.colls: - mountHitMaram = strategy.divest(type()(uint266).max) (contracts/BaseVault.sol#287)
	State variables written after the call(s): - maxlockeBrofit = a didal - amountWindgrawn (contracts/BaseVault.sol#267)
	- totalStrategWeldings -= oldBal (contracts/BaseVault.sol#259) cy in BaseVault,withdrawFromStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#362-376): External calls:
	- amountWithdrawn = strategy.divest(tokenAmount) (contracts/BaseVault.sol#864) State variables written after the call(s): - artragis(strategy).balance = amountWithdrawn (contracts/BaseVault.sol#866)
	- strategyia(strategy).balance -= amountWithdrawn (contracts/BaseWault.so.M9366) - totalStrategyMoldings -= amountWithdrawn (contracts/BaseWault.so.M9371) - https://github.com/crytic/sithber/wiki/Detector-DocumentationFreentrancy-vulnerabilities-2
Reentran	cy in L2YaultL112Rebalance(bool,uint256) (contracts/polygon/L2Yault.sol#527-538):
	External colls: liquidate(amount) (contracts/polygon/L2Vault.sol#551) - amount%ithdrawn = strateav.divestf(okenAmount) (contracts/BaseYault.sol#364)
	<pre>_ acountWithdram = strategy.dives[(tokenAmount) (contracts/BaseVault.sol#364) _ transfeToll(amountToBand) (contracts/polygon/(2Vault.sol#364) - bridgeSteros.l2dH(draw(amount)) (contracts/polygon/LXVault.sol#543)</pre>
	- L2Wormhol#Bourdr(wormhol#Bourdr).reportTransferredFund(amount) (contracts/polygon/L2Wault.sol#552) Event emitted after the call(s): - TransferToLLimount) (contracts/polygon/L2Wault.sol#544)
	transferToL1(amountToSend) (contracts/polygon/L2Vault.solE538) cy in L2Vault, divestFonLiu(init266) (contracts/polygon/L2Vault.solE557-566):
Reentrar	
	External calls: ChormholdBoutsr(wrshnlaRoutsr).requestFunds(amount) (contracts/polygon/L2Vault.sol#558)

- bridgeEscrow.l2Withdraw(amount) (contracts/polygon/L2Vault.sol#543) Event emitted after the call(s): - Transferful amount)

ter the call(s): mount) (contracts/polygon/L2Vault.sol#544) depositIntoStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#323-339)

External calls: - stratego:invest(tokenAmount) (contracts/BaseVault.sol#337) Event emitted after the call(s): - Stratego@positistratego:tokenAmount) (contracts/BaseVault.sol#338) ncy in EmergencyWithdrawalQueue.dequeue() (contracts/polygon/EmergencyWithdrawalQueue.sol#79-94):

- 9ftretegyDepDit(ftretagy\_tclankBourt) (contracts/polygon/EmergencyWithdrawalQueue.sol#79-94): External calls: - redesedSextMount = vult.redeemByEmergencyWithdrawalQueue(headPtr,withdrawalRequest.shares,withdrawalRequest.recsiver,withdrawalRequest.comer) (contracts/polygon/EmergencyWithdrawalQueue.sol#86-87) Event weitted after the calls): may in EmergencyWithdrawalQueue(headPtr,withdrawalQueue(headPtr,withdrawalRequest.shares,withdrawalRequest.recsiver,withdrawalRequest.comer) (contracts/polygon/EmergencyWithdrawalQueue.sol#86-87) may in EmergencyWithdrawalQueue.sol#80-41) may in EmergencyWithdrawalQueue.sol#80+41 external calls: - redesedSextAount = vult.redeemByEmrgencyWithdrawalQueue.sol#70+40 Event exitted after the call(s): - redesedSextAount = vult.redeemByEmrgencyWithdrawalQueue.sol#70+40 Event exitted after the call(s): - redesedSextAount = vult.redeemByEmrgencyWithdrawalQueue.sol#180+182 Event exitted after the call(s): - External calls: - redesedSextAount = vult.redeemByEmrgencyWithdrawalRequest.shares) (contracts/polygon/EmergencyWithdrawalQueue.sol#180+182) Event exitted after the call(s): - External calls: - External calls: - vult.br/dotaewalQueuew(headPtr,withdrawalRequest.comer,withdrawalRequest.shares) (contracts/polygon/EmergencyWithdrawalQueue.sol#180+112) mary in [carByEndPherencewalRequeueWithdrawalQueue.sol#180+112) Event exitted after the call(s): - External calls: - vult.br/dotaewalQueuewalRequeueWithdrawalQueue.sol#180+112) Event exitted after the call(s): - vult.br/dotaewalQueuewalRequeueWithdrawalQueue.sol#180+112) Event exitted after the call(s): - vult.br/dotaewalQueuewalRequeueWithdrawalQueue.sol#180+112) Event exitted after the call(s): - vult.br/dotaewalQueueWithdrawalQueue.sol#180+112) - vult.br/dotaewalQueueWithdrawalQueue.sol#180+112) - vult.br/dotaewalQueueWithdrawalQueue.sol#180+112)

External calls: - vaul.tridgeExrow().12ClaerFund(smount) (contracts/polygon/L2WoreholeRouter.sol#64) Event emitted after the call(s): - transferFound(smount) (contracts/polygon/L2WoreholeRouter.sol#65) ancy in BaseVaul.twithfrawFromStrategy(BaseStrategy,uint266) (contracts/BaseVaul.sol#362-376): External calls: - amountWithdrawFromStrategy(BaseStrategy,uint266) (contracts/BaseVaul.sol#362-Forth emitted after the call(s): - StrategyWithdrawAltrategy,amountWithdrawN (contracts/BaseVaul.sol#374) - StrategyWithdrawAltrategy,amountWithdrawN (contracts/BaseVaul.sol#374) - https://github.com/cyticl/sliters/ski/WatesTor-DorumentationFromTrans-vulnerabilities-3

ult.harves(18as6trateq()) (contracts/BaseVault.acl#487-462) uses timestamp for comparisons Dangerous comparisons: - requirs(bool,string)(block.timestamp >= lastHarvest + lockInterval,PRDFT\_UNLOCUND) (contracts/BaseVault.scl#499) Ult.lockedProfil() (contracts/BaseVault.scl#447-55 uses timestamp for comparisons Dangerous comparisons: Dangerous comparisons: monitories (contracts/Dangerous) (contracts/BaseVault.scl#449) monitories (contracts/Dangerous) (contracts/Dangerous) (contracts/BaseVault.scl#449) monitories (contracts/Dangerous) (contracts/Dangerous) (contracts/BaseVault.scl#449) monitories (contracts/Dangerous) (contracts/Dangerous) (contracts/BaseVault.scl#449) Dangerous comparisons (contracts/Dangerous) (contracts/Dangerous

.lockadTV(1) (contractPdpJgbn/Ld7Wull Prince (contracts/pplygon/L2Vault.sol#469) dDangerous comparisons: - block.tmestamp >= lostTV(Update + lockInterval (contracts/pplygon/L2Vault.sol#469) destalledPrior((contracts/pplygon/L2Vault.sol#600-684) uses timestamp for comparisons Discornes comparisons:

Dangerous comparisons: - totalSupply() > 0 (contracts/polygon/L2Vault.sol#582) :ce: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp

MulticalLoulticalL(bytes[]) (contracts/external/MulticalLoul#=27) uses assembly - INLINE ASM (contracts/external/MulticalL.oll#=2-21) Reference: https://github.com/crytis/slither/wiki/Detector=Documentationassembleum

sressor 0.313 (contract/strindersrelbs.col2) necessites a version to recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Consider deploying with 0.4.12/0.7.0/0.8.7
ps version 0.4.33 (contract/strindersrelbs.col2) necessites a version too recent to be trusted. Cons

0.6.12/0.7.6/0.8.7 deploying with 0.6.12/0.7.6/0.8.7 .6.12/0.7.6/0.8.7 ng with 0.6.12/0.7.6/0.8.7

Variable BaseVault.swapWithdrawalQuuueIndexes(uint256,uint256).newStrategy1 (contracts/BaseVault.sol#31) is too similar to BaseVault.swapWithdrawalQueueIndexes(uint256,uint256).newStrategy2 (contracts/BaseVault.so Variable Constants.L1\_LND\_TRANSFER\_REPORT (contracts/Constants.sol#21) is too similar to Constants.L2\_ENQ\_TRANSFER\_REPORT (contracts/Constants.sol#7) References https://github.com/cyrii/siliter/xyii/Detecto-focumentationAryimabe-maes-are-too-imilar

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable
BaseStrategy (contracts/BaseStrategy.sol#9-48) does not implement functions:
<ul> <li>BaseStrategy.balanceOfAsset() (contracts/BaseStrategy.sol#25)</li> </ul>
- PaseStrategy divect(wipt264) (contracts/PaseStrategy col#26)

BridgeEscrow.vaultNonce (contracts/BridgeEscrow.sol#19) should be constant Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

#### BridgeEscrow.vaultNonce (contracts/BridgeEscrow.sol#19) should be constan Reference: https://github.com/crytic/slither/wiki/Detector-Decumentation#

<ul> <li>BaseVault.asset() (contracts/BaseVault.sol#33-35)</li> </ul>
- L2Vault.asset() (contracts/polygon/L2Vault.sol#149-151)
multicall(bytes[]) should be declared external:
<ul><li>– Multicall.multicall(bytes[]) (contracts/external/Multicall.sol#9-27)</li></ul>
linkVault(L2Vault) should be declared external:
<ul> <li>EmergencyWithdrawalQueue.linkVault(L2Vault) (contracts/polygon/EmergencyWithdrawalQueue.sol#48-57)</li> </ul>
totalDebt() should be declared external:
<ul> <li>EmergencyWithdrawalQueue.totalDebt() (contracts/polygon/EmergencyWithdrawalQueue.sol#65-67)</li> </ul>
initialize(address, ERC20, address, BridgeEscrow, EmergencyWithdrawalQueue, address, uint256, uint256, uint256[2]) should be declared external:
- L2Vault.initialize(address, ERC20, address, BridgeEscrow, EmergencyWithdrawalQueue, address, uint256, uint256, uint256[2]) (contracts/polygon/L2V
convertToShares(uint256) should be declared external:
<ul> <li>L2Vault.convertToShares(uint256) (contracts/polygon/L2Vault.sol#335-337)</li> </ul>
convertToAssets(uint256) should be declared external:
<ul> <li>L2Vault.convertToAssets(uint256) (contracts/polygon/L2Vault.sol#356-358)</li> </ul>
previewRedeem(uint256) should be declared external:
- L2Vault.previewRedeem(uint256) (contracts/polygon/L2Vault.sol#391-393)
maxDeposit(address) should be declared external:
- L2Vault.maxDeposit(address) (contracts/polygon/L2Vault.sol#413-416)
maxMint(address) should be declared external:
<ul> <li>L2Vault.maxMint(address) (contracts/polygon/L2Vault.sol#419-422)</li> </ul>
maxRedeem(address) should be declared external:
<ul> <li>L2Vault.maxRedeem(address) (contracts/polygon/L2Vault.sol#425-427)</li> </ul>
maxWithdraw(address) should be declared external:
<ul> <li>L2Vault.maxWithdraw(address) (contracts/polygon/L2Vault.sol#430-432)</li> </ul>
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external

# src/AffineGovernable.sol

Progra version*0.8.13 (contracts/AffineGovernable.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0. Sol=0.8.16 is not recommended for deployment Reference: Hoss/J(thub.come(trytic/alther/stki/Detector-Documentation#incorrect-versions-of-solidity		
AffineGovernable.governance (contracts/AffineGovernable.sol#6) should be constant		

#### src/BaseStrategy.sol

Reference: https://github.com/crytic/slither/wiki/Detector-Documentation/#payable-functions-using-delegatecall-inside-a-loop	

aseStrategy,vault (contracts/BaseStrategy.sol#13) is never initialized. It is used in:	
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-state-variable	

cy in Ba

is: Mirrost = stratogy.totallockdWilw() (contracts/BaseVault.sol#432) as written after the call(s): stratogy.balancs = balancs/hisHarvest (contracts/BaseVault.sol#435) thub.com/crytics/silther/rdki/Datector-Documentation#reentrancy-vulnerabilities-1

whithdrawalQueum().offset (contracts/BaseYault sol#219) is a local variable never initialized 6().mountsToInvest (contracts/BaseYault.sol#556) is a local variable never initialized BaseStateg()).totalPortikterumg (contracts/BaseYault.sol#2160) is a local variable never in /github.com/crytic/slither/wski/Datector-Documentationfuninitialized-local-wariables nitialized ariable never initialized riables

BaseVault.rebalance() (contracts/BaseVault.sol#509-598) ignores return value by strategy.divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol#567) Reference: https://github.com/cryTie/siltMarkel/ablumationAmussed-Teturn

ccess,result) = address(this).delegatecall(dat(i)) (contracts/sternal/Multicall.scl#12) amountiithdram = strategy.divect(type()(uint260.max)(contracts/BaseAvult.scl#257) math.min.amountToToTwest, asset.balanceOf(address(this))) (contracts/BaseAvult.scl#253) invest(amountToToTwest, asset.balanceOf(address(this))) (contracts/BaseAvult.scl#2563) = strategy.total.orkedValue() (contracts/BaseAvult.scl#2565) curfStrategyTVL (dostarts/BaseAvult.scl#2567)

Event emitted after the call(s): . Stritegydepsit(trategy,teknowunt) (contracts/BaseVault.sol#380) Beentrany in BaseVault.withdrawFromStrategy/UBaseStrategy,uint256) (contracts/BaseVault.sol#362-376): Efetterant calls: - amountWithdrawn - strategy.divest(tokenAmount) (contracts/BaseVault.sol#364) Event emitted after the call(s): - StrategyWithdrawal(strategy,amountWithdrawn) (contracts/BaseVault.sol#376) Reference: Thttp://githuk.com/grit/GiltBrefer.WithDectorco-commentionmentare.revulnerabilities-3
BaseVall.harvat(BaseKrategy[]) (contracts/BaseVault.sol#497-642) uses timestamp for comparisons Deprevous comparisons - require(Bool,string)(block.timestamp >= lastHarvest + lockInterval,PROFT_UNLOCKING) (contracts/BaseVault.sol#649) BaseVault.lockEdForti() (contracts/BaseVult.sol#64-75) uses timestamp for comparisons Dangerous comparisons Beforence: https://github.cont/estic/alsterval.(contracts/BaseVault.sol#649)
<pre>wetters: https://giunotumotycic/interpretations/color-potential/wetters/app Multicall.multicall.ptyst[]) (contract/systemal/wulticall.sols9-27) uses assebly - NULRE ASM (contract/systemal/wulticall.sols92-23) Befrement: https://github.contract/systemal/wulticall.sols92-33</pre>
BaseVault.removeStrategy (BaseStrategy) (contracts/BaseVault.sol#240-271) has costly operations inside a loop: - totalBgs - stratinfo.tvlBgs (contracts/BaseVault.sol#240-271) has costly operations inside a loop: - totalBtategyPidimgs - sidBal (contracts/BaseVault.sol#240) BaseVault.removeStrategy(BaseStrategy) (contracts/BaseVault.sol#240) BaseVault.removeStrategyDiloxEin
BasYwult, liquidnet(sist256) (contract/BasVult,s014646-253) is never used and should be removed BasYwult-depositIntEstrategies) (contracts/BasVult,so14646-233) is never used and should be removed BasYwult-diffuseTonEstrategies(intEstrategies(intEst)) (and the state of the state
Pragma version% 8.812 (contracts/Affinationermable sol2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.813 (contracts/AssGrareage,nel2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.313 (contracts/AssGrareage,nel2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.313 (contracts/AssGrareage,nel2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.313 (contracts/AssGrareage) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.313 (contracts/AssGrareage) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 8.313 (contracts/AssGrareage) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 0.8.313 (contracts/AssGrareage) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 0.8.313 (contracts/AssGrareage) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 0.8.313 (contracts/AssGrareage) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 0.8.313 (contracts/interface/Nac(Tabadomaper.col2)) necessitates a version too recent to be trusted. Consider deploying with 0.6.2.6/0.7.6/0.8.7 Pragma version% 0.8.312 (contracts/interface/Nac(Tabadomaper.col2)) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 0.8.312 (contracts/interface/Nac(Tabadomaper.col2)) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 Pragma version% 0.8.312 (contracts/interface/Nac(Tabadomaper.col2)) necessitates a version too recent to be trusted. Consider deploying with 0.6.2.2/0.7.
Low level call in Multicall.Multicall(bytes[]) (contracts/wsternal/Multicall.sol#9-27): - (success.result) = address(this).delagatecall(data[i)) (contracts/wsternal/Multicall.sol#12) Reference: Thtp://githuk.comtorytic/allther/mili/Destero-comentalionalDest-level-calls
Variable BaseVault.swapWithdrawalQueueIndexes(uint256,uint256).newStrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.swapWithdrawalQueueIndexes(uint256,uint256).newStrategy2 (contracts/BaseVault Reference: https://github.com/crytic/slither/wiki/Detactor-Documentation#variable-names-are-too-similar
BaseStrategy (contracts/BaseStrategy.so/AP-48) does not implement functions: — BaseStrategy.halmocOffster() (contracts/BaseStrategy.so/APS) — BaseStrategy.invest(unit26) (contracts/BaseStrategy.so/APS) — BaseStrategy.invest(unit26) (contracts/BaseStrategy.so/APS) — BaseStrategy.invest(softafbrategy.so/APS) Merrence: https://githuk.contracts/BaseStrategy.so/APS)

BridgeEscrw.vaultNonce (contracts/BridgeEscrw.sol#19) should be constant VormholeAoutr.narvialBNonce (contracts/BridgeEscrw.sol#19) should be constant NormholeAoutr.narvialBNonce (contracts/NormholeRoute.sol#15) should be constant NormholeAoutr.otheriuy=Rohuind (contracts/NormholeRoute.sol#13) should be constant

# src/BaseVault.sol

Multerine: mitroi/jottes/j/centroi/witroi/siteri/witroi/siteri/witroi/siterine/site
BaseStrategy.vault (contracts/BaseStrategy.solF13) is never initialized. It is used in: - BaseStrategy.seegEECC00 (contracts/BaseStrategy.solF43) is never initialized. It is used in: BaseStrategy.setE (contracts/BaseStrategy.solF13) is never initialized. It is used in: AffineGovernable.governamecs (contracts/AffineGovernables.solF64) is never initialized. It is used in: WornholeRouter, validstewernableRoter.solF34) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF44) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF44) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF44) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF44) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF44) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF45) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55) is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55 is never initialized. It is used in: - WornholeRouter, validstewernableRoter.solF55
BaseYault.rebilance() (Contracts/BaseYault.sol#549-590) uses a dangerous strict equality: - anountFlowest ⇒ 0 (contracts/BaseYault.sol#584) Reference: https://github.com/cryii/silhut=sol=Co-Documentation#dangerous-strict-equalities
Reentrancy im BaseVault-harvest(BaseStartegy(1)) (contracts/BaseVault.sol#407-442): External calls: - balanceThisMarvest = strategy,totalLookedVauk() (contracts/BaseVault.sol#632) State variables writen after the call(s): - strategies(strategy).balance = balancihisMarvest (contracts/BaseVault.sol#435) Reference: https://github.certy.ti/s/literst-co-baumentation#resting-vulnerabilities-1
BasYull-harvest(BasStrateg()).totalProfitacrud (contract/BasYull.a014638) is a local variable never initialized BasYull-reprinzetindramyUnow().offset (contract/BasYull.sol2470) is a local variable never initialized BasYull-rebiance().mamuntScInvest (contract/BasYull.sol2450) is a local variable never initialized Reference: inter/julluc.doc/pris/ilitartet/BasYull.sol2450) is a local variable never initialized
BaseVault.rebalance() (contracts/BaseVault.sol#640-890) ignores return value by strategy.divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol#667) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
BaseVault.baseInitialize(address_ERCDA_address_BriggEscrem).poversmanse (contracts/BaseVault.sol#37) lacks a zero-check on : 
<pre>WelticalLinglica</pre>
Reentranty in BaseWull treeweStrategy(BaseStrategy) (contracts/BaseVault.sol#260-273): = amountWithdram = strategy.divart(type()(uint260.max) (contracts/BaseVault.sol#267)) State variables writen after the coll610: = mainSchedFordfile=OldBal = mountWithdram (contracts/BaseVault.sol#267) Reentrany: In SetVault.sol#2007(iii) (contracts/BaseVault.sol#267) External colle: = mainSchedFordfile=OldBal = mountWithdram (contracts/BaseVault.sol#267) External colle: = mainSchedFordfile=OldBal = mountWithdram (contracts/BaseVault.sol#266) State variables writen after the coll63) = totalStatespidlafuegy = mountWithdram (contracts/BaseVault.sol#266) = totalStatespidlafuegy = mountWithdram (contracts/BaseVault.sol#266) = totalStatespidlafuegy = mountWithdram (contracts/BaseVault.sol#267) Reference: https://github.com/crytic/lither/aki/Statestor-OcumentAtiomStatestor-Outpacts/BaseVault.sol#270) Reference: https://github.com/crytic/lither/aki/Statestor-OcumentAtiomStatestor-Outpacts/BaseVault.sol#270)
Reentrany in BaseVault.deposiIntoStrategy(BaseStrategy,uint256) (contracts/BaseVault.sol#323-339): External calls: - strategy.invest(tokeAmount) (contracts/BaseVault.sol#337)

Event emitted after the call(s): - StrategyDeposit(strategy,tokenAmount) (contracts/BaseVault.sol#362-376): Beentrancy im BaseVault.michter#cmsStrategy(BaseStrategy,uint366) (contracts/BaseVault.sol#362-376):
External calls: — amountWithdrawn = strategy.divest(tokenAmount) (contracts/BaseVault.sol#364) Event emailted after the call(s):
- StrategyWithdrawal(strategy,amountWithdrawn) (contracts/BaseWault.sol#374) Beference: https://github.com/crytic/Silther/wiki/Detector-Documentation#reentrancy-wulnerabilities-3
lasY4ult.harves(lassEtatagy()) (contracts/BaseVault.s0]#407-462) uses timestamp for comparisons Dengretous Generations:
— require(boo),string)(block,tiestamp >= lastWarvest + lockInterval,PROFIT_UMLOGKING) (contracts/BaseVault.sol#469) laseVault.lockedProfit() (contracts/BaseVault.sol#468-475) uses timestamp for comparisons Danaerous comparisons:
<pre>- block.timestamp &gt;= lastHarvest + lockInterval (contracts/BaseVault.sol#669) leference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp</pre>
Wlticall.multicall(bytes[]) (contracts/external/Wulticall.sol89-27) uses assembly — THLTNE ASM (contracts/external/Wulticall.sol89-23) Merrance: https://oithub.com/cryst/cialltar/swiki/Datector-Documentation#assembly-usage
laseVault.removeStrategy(dsasStrategy) (contracts/BaseVault.sol#240-271) has costly operations inside a loop:
<ul> <li>totalBps == stratInfo.tvlBps (contracts/BnavYault.sol#240)</li> <li>laseVault.removeStrategy(BaseStrategy) (contracts/BaseVault.sol#240-271) has costly operations inside a loop:</li> <li>totalStrategy(BaseStrategy) = oldBal (contracts/BaseVault.sol#250)</li> </ul>
lastVall.removStrategy/GauSTrategy/Contracts//BastVall.sol2240-272) has costly operations inside a loop: - maiocekepfoit = - SidBal - menoutHindram(contract/AssVall.sol2247)
las¥Vuli.updat6StrategyAllocations(BaseStrategy[],uint256(]) (contracts/BaseVault.sol#278-207) has costly operations inside a loop: - totalbps -= oldBps (contracts/BaseVault.sol#293)
savývult, increasofVLB9S(vint26) (contracts/BaseVult.salr204-210) has cotly operations inide a loop: - totalbeg memofcalBpg (contracts/BaseVult.salr204-210)
leference: https://github.com/cryti//slither/wiki/Detector-Documentation≢costly-operations-inside-a-loop MaseYault. liquidate(uint256) (contracts/BaseYault.sc)#496-525) is never used and should be removed
Marvais, ildusertuoto tontintos tentrovalais antenna una monta una monta se revere Marvais, depositintoittat y (Baseltat y, ulatis) (contracts /Baseluult.ol#23-339) is never used and should be removad marvais. Apositintoittat y (Baseltat y, ulatis) (contracts /Baseluult.ol#23-339) is never used and should be removad marvais. Marvais for the sensitive for the sensitive sensitive sensitive sensitive sensitive sensitive sensitive for the formation of the sensitive
rapma variant8.8.13 (contract/Affindeowarable sol87) necessitates a variant too recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/MassGtratop, variable) necessitates a variant too recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/MassGtratop, variable) necessitates a variant too termeted be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/MassGtratop, variable) necessitates a variant too termeted be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/VariableSuter.sol27) necessitates a variant too termete to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/VariableSuter.sol27) necessitates a variant too termete to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/VariableSuter.sol27) necessitates a variant too termete to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/VariableSuter.sol27) necessitates a variant too termete to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/VariableSuter.sol27) necessitates a variant too termete to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 rapma variant8.6.13 (contract/Interface/INDIChiaInMarger.sol27) rapma variant8.6.13
oli-0.8.16 is not recommended for deployment afference: https://github.com/styrid/silther.wiki/Detector-Documentation#incorrect-versions-of-solidity
ow level call in Multicall.multicall(bytes()) (contracts/seternal/Multicall.sol#9-27): - (success.result) = address(this).dolegatacall(data(1)) (contracts/seternal/Multical.sol#12) eference: https://github.contracts/iolitalretar/seventations/ab=/seventa-calls
ariable BaseVault.swapHithdrawalQueueIndexes(uint256,uint256).newStrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.swapHithdrawalQueueIndexes(uint256,uint256).newStrategy2 (contracts/BaseVault. Weference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
<pre>sasStrategy (untracting solf==40) dem not implement functions:</pre>
iridgeEscrow.waultNonce (contracts/BridgeEscrow.sol#19) should be constant NormholBenter.nevtValiBNonce (contracts/NormholBenter.sol#15) should be constant NormholBenter.sol#100 (constant/NormholBenter.sol#15) should be constant

# src/BridgeEscrow.sol

https://github.

Multicality Multicality (Multicality) (Multi
BaseStrategy.vault (contracts/BaseStrategy.solF13) is never initialized. It is used in: - BaseStrategy.seep(ECCP) (contracts/BaseStrategy.solF43-47) BaseStrategy.seep(Contracts/BaseStrategy.solF43) is never initialized. It is used in: AffindEovernbls.pupermance (contracts/AffindEovernbl48.solF64) is never initialized. It is used in: WornbulRPouter.valEdtectronouter.valEdtectronouter.valEdtectronouter.solF44-45) NornbulRPouter.valEdtectronouter.valEdtect
BaseVault-rebalance() (contracts/BaseVault-acl#EGA-580) uses a dangerous strict equality: - a souvent Torvest = 0 (contracts/BaseVault-sa)#ESA) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dangerous-strict-equalities
Reentrancy im BasWault-haress(BasStatsgy(1) (contracts/BassVault.solf467-662): Extrant lealls: - balanceThisHarest = strategy.totallockedVaus() (contracts/BaseVault.solf452) State variables writen after the call(s): - strategies(strategy).balance = balanceThisHarest (contracts/BaseVault.solf435) Reference: http://ditub.com/pris/i/ilitetto-Documentation/renerabilities-1
BassWalltrebilaned/JamountsToInvest (contracts/BassWallts01656) is a local variable never initialized BassWallt_nvest(BassStratego)().httpl?fottActorund (contracts/BassWallts01458) is a local variable never initialized BassWallt_organizeWithdTamaDQuuw().offset (contracts/BassWallts01229) is a local variable never initialized Reference: intpl://githdt.com/grtis/jithtreta/BassWallts01229) is a local variable never initialized
BaseVault.rebalance() (contracts/BaseVault.sol#549-590) ignores return value by strategy.divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol#567) Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
BaseVault.baseInitializeidadress_ERC20_siddress_BridgeEstrom.governames (contracts/BaseVault.sol#37) lacks a zero-check on : - govername = governames (contracts/BaseVault.sol#27) BaseVault.baseInitializeidadress_ERC20_siddress_BridgeEstrom, JonarbalkAult.sol#37) lacks a zero-check on : - wormbidRewture = governameStature (contracts/BaseVault.sol#37) lacks a zero-check on : - commer = _ommer (contracts/BaseVault contracts/BaseVault.sol#32) lacks a zero-check on : - commer = _ommer (contracts/BaseVault.sol#28) BridgeEstrow.initialize(address_IROstDhainAmanger), vult (contracts/BridgeEstrow.sol#32) lacks a zero-check on : - wormbidRewture = BaseVault(gestrow.sol#28) BridgeEstrow.initialize(address_IROstDhainAmanger), vult (contracts/BridgeEstrow.sol#30) - wormbidRewture = BaseVault(gestrow.sol#30) Areference: http://glithub.com/cont/BridgeEstrow.sol#30) Areference: http://glithub.com/cont/BridgeEstrow.sol#30) - wormbidRewture = BaseVault(Jowett-DecommentIonMestimg-zero-address-ulldation
<pre>Relicial.mitcali(pres()) (contracts/asternal/Walicali.sol89-20) has esternal calis inside a long: increas_result) = address(thin.dalogsteral)(deti(i)) (contracts/asternal/Walicali.sol812) BestWalt.mergetStategr(SentExtep) (contracts/BestWalt.sol849-42) has esternal calis inside a long: harmont/intrage a string prise()(unt55). BestWalt.mergetStategr(SentExtep) (contracts/BestWalt.sol849-42) has esternal calis inside a long: harmont/intrage.string.collaboker/Aun().contracts/BestWalt.sol8432) BestWalt.mergetStategr(SentExtep) (contracts/BestWalt.sol849-42) has esternal calis inside a long: harmont infraeres.string.collaboker/Aun()) (contracts/BestWalt.sol8432) BestWalt.reblance() (contracts/BestWalt.sol8450-59) has esternal calis inside a long: string.comtToNvest = Mth.nifesontToNvest, seet.balance()(contracts/BestWalt.sol8583) BestWalt.reblance() (contracts/BestWalt.sol856-599) has esternal calis inside a long: string.comtToNvest = Mth.nifesontToNvest = Nth.nifesontToNvest = Nth.nifesontToNvest</pre>
Reentrancy in BaseVault.reseveStrategy(BaseStrategy) (contracts/BaseVault.sol#240-271): Entrance Scale: - amountWithdram = strategy.divert(type()(uint256).max) (contracts/BaseVault.sol#267) State variables written strot the cill(s): - maxlackedFordit+= oldBal - amountWithdram (contracts/BaseVault.sol#267) - totalStrategyNolBing == oldBal (contracts/BaseVault.sol#260) Reentrancy in BaseVault.sthtDramFordStrategy(BaseStrategy.uint256) (contracts/BaseVault.sol#262-376): Extern of contracts/BaseVault.sol#250 State variables written affort the cill(s): - strategiesIstrategyNolBings == sountWithdram (contracts/BaseVault.sol#260) - totalStrategyNolBings == sountWithdram (contracts/BaseVault.sol#271) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273) Reference: http://githUnt.com/strit/BaseVault.sol#273-339): _ strategy.invest(tokenAmount) (contracts/BaseVault.sol#37)

Fund:smithed_sfort.thc.call(s):         - Statespythonististatespythonistatespythespythonistatespythonis
BastYault.harvet(BastStringy()) (contracts/BastYault.sol#407-462) uses timestamp for comparisons Dangerous comparisons) — require(box],string)(block.timestamp >= lastHarvet + lockInterval,PMDTT_ULUCKIND) (contracts/BaseYault.sol#409) BasYault.clocketDroft() (contracts/BastYault.sol#464-75) uses timestamp for comparisons Dangerous comparisons Dangerous comparisons Dangerous comparisons Dangerous try(rytic)(silterVat()Detect)-Comparisons(State) Parsons: http://sithub.com/privis/silterVat()Detect-Comparisons(State) Dangerous try(rytic)(silterVat()Detect)-Comparisons(State) Dangerous try(rytic
Multicall.multicall(bytes[]) (contracts/external/Multicall.solM9-27) uses assembly - NUNE ASM (contracts/external/Multicall.solM9-23) Reference https://github.com/cyr/iciallume/sixi/Detector-Documentation#assembly-usage
BasYabilt:removeStrategy) (SasStrategy) (contract/BasYabilt:s01254) - tot318p - stratfor/cubbs (contract/BasYabilt:s01254) BasYabilt:removeStrategy)(SasStrategy) (contract/BasYabilt:s01254) - tot318trategy)(BasStrategy) (contract/BasYabilt:s01254) BasYabilt:removeStrategy)(SasStrategy) (contract/BasYabilt:s01254) BasYabilt:removeStrategy)(BasStrategy) (contract/BasYabilt:s01254) BasYabilt:removeStrategy)(SasStrategy) (contract/BasYabilt:s01254) BasYabilt:removeStrategy)(SasStrategy) (contract/BasYabilt:s01254) BasYabilt:removeStrategy)(SasStrategy) (contract/BasYabilt:s01257) BasYabilt:removeStrategy)(SasStrategy) (contract/BasYabilt:s01257) BasYabilt:removeStrategy)(SasStrategy)(contract/BasYabilt:s01257) BasYabilt:removeStrategy)(SasStrategy)(contract/BasYabilt:s01257) BasYabilt:removeStrategy)(SasStrategy)(contract/BasYabilt:s01257 BasYabilt:removeStrategy)(SasStrategy)(contract/BasYabilt:s01257 BasYabilt:removeStrategy)(SasStrategy)(contract/BasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/BasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/BasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/BasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/BasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/SasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/SasYabilt:s01257 - contractStrategy)(SasStrategy)(contract/SasYabilt:s01257 - contractStrategy)(contract/SasYabilt:s01257 - contractStrategy)(con
Basivalit, liquidsteluitit550) (contractor/Basivalit.sa/8456-252) is nover used and should be removed Basivalit.demostitetetetetetetetetetetetetetetetetetet
Pragma version 0.1.1 (contracts/dfindovernable.sol2) necessitates a version ton scenent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to scenent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/metrics/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.4/0.8.7 Pragma version 0.8.11 (contracts/destides/metrics/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 Pragma version 0.8.11 (contracts/interio/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 Sol2-0.8.15 (contracts/interio/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7 Sol2-0.8.16 (contracts/interio/sol2) necessitates a version to recent to be trusted. Consider deploying with 0.4.12/0.7.6/0.8.7
Low level call in Multicall.multicallbytes()) (contracts/external/Multicall.sol#9-27): - [success_result] = address(this).delagtecall(data(i)) [contracts/external/Multicall.sol#12) Reference: http://github.adv/cryiti/silter#xiv/Multicall.sol#9-21]s
Variable BaseVault.swapHithdrawslQueueIndexes(uint256,uint256).newStrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.swapHithdrawslQueueIndexes(uint256,uint256).newStrategy2 (contracts/BaseVault.so Reference: https://github.com/crytic/slither/wiki/Batector-Documentation#variable-names-are-too-similar
BaseStrategy (contracts/BaseStrategy,sol#9-48) does not implement functions: - BaseStrategy: LabaneoDfAses() (contracts/BaseStrategy.sol#35) - BaseStrategy: Lones(Lunt256) (contracts/BaseStrategy.sol#36) - BaseStrategy: LotalLockedValue() (contracts/BaseStrategy.sol#31) Reference: http://github.com/cryii/silter#ii/Unetcot=Commentation#nimplemented-functions
BridgeEcrow vallburgs (santrat/BridgeEsrow,sal149) shuld be constant WormbleRouter.chmrtaygeThainG (contrats/WormholsRouter.sol15) shuld be constant WormbleRouter.chmrtaygeThainG (contrats/WormholsRouter.sol15) shuld be constant MormbleRouter.chmrtaygeThainG (contrats/WormholsRouter.sol15) shuld be constant Reference: https://github.com/cryti/silthut/wiki/Detector-Documentation#istate-variables-that-could-be-declared-constant

#### src/Constants.sol

Pragma version%8.5.8 (contracts/Constant.sold2) necessitates a version too recent to be trutted. Consider deploying with 0.6.12/0.7.6/0.8.7 sol2-0.8.16 is not recommended for deployment Reference: https://github.com/cryiic/siliner/wiki/Detector-Documentation#incorrect-version=-of=solidity Versible Constants.11 BMD TAMESFE BEDDET (contracts/Constants.eole12) is no visible no fonctants.2 RMD TAMESFE BEDDET (contracts/Constants.

# src/DollarMath.sol

Pragma version\*0.6.13 (contracts/DollarMath.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 solc-0.8.1.6 is not recommended for deployment Reference: http://githb.com/cyrtic/silter/wiki/Detector-Documentation#incorrect-versiona-of-solidity

# src/WormholeRouter.sol

Multicall.multicall(bytes[]) (contracts/external/Mu	ulticall.sol#9-27) has delegatecall inside a loop in a payable function: (success,result) = address(this).delegatecall(data[i]) (contracts/external/Multicall.sol#12 Detector=Documentation/#payable=functions=using=delegatecall=inside=a=loop
Reference: https://github.com/crytic/slither/wiki/[ BaseStrategy.vault (contracts/BaseStrategy.sol#13)	
<ul> <li>BaseStrategy.sweep(ERC20) (contracts/Base BaseStrategy.asset (contracts/BaseStrategy.sol#21)</li> <li>BaseStrategy.reconfEPC20) (contracts/Base</li> </ul>	<pre>intvor initialized. It is used in: dfurtery.sol#d3-47) is never initialized. It is used in: dfurtery.sol#d3-47) able.sol#d3 is never initialized. It is used in: able.sol#d3 is never initialized. It is used in: initialized.able.sol#d3 is never initialized.able.sol#d4-45) able.sol#d3 is never initialized.able.sol#d4-45) able.sol#d4 is never initialized.able.sol#d4 is never able.sol#d4 is never able.sol#d4</pre>
<ul> <li>BaseStrategy.sweep(ERC20) (contracts/Base</li> <li>AffineGovernable.governance (contracts/AffineGovern</li> <li>wormholeRouter.otherLayerRouter (contracts/Wormhole</li> </ul>	Decleugy-solans-w/) mable.sol80 is newer initialized. It is used in: Router.sol813) is newer initialized. It is used in:
<ul> <li>WormholeRouter_validateWormholeMessageEn WormholeRouter.otherLayerChainId (contracts/Wormhol WormholeRouter_validateWormholeMessageEn</li> </ul>	nitter(Worshole.VM) (contracts/WorsholeRouter.sol#41-45) leRouter.sol#14) is never initialized. It is used in: niter(Worshole.VM) (contracts /worsholeRouter.sol#11.45)
<ul> <li>WormholeRoutervalidateWormholeMessageEn WormholeRouter.nextValidNonce (contracts/WormholeRo WormholeRoutervalidateWormholeMessageEn</li> </ul>	Mitter(INformhole.VW) (contracts/NormholeRouter.sol#A1-45) mitter(INformhole.VW) (contracts/NormholeRouter.sol#A1-45)
- amountToInvest == 0 (contracts/BaseVault.sol#B49- - amountToInvest == 0 (contracts/BaseVault. Reference: https://github.com/crytic/slither/wiki/[	590) uses a dangerous strict equality: .rol#584) Detector-Documentation#dangerous-strict-equalities
Reentrancy in BaseVault.harvest(BaseStrategy[]) (co External calls:	
<ul> <li>balanceThisHarvest = strategy.totalLocket</li> <li>State variables written after the call(s):</li> <li>strategies[strategy].balance = balanceThi</li> </ul>	dValue() (contracts/BaseVault.sol#432)
<ul> <li>strategies[strategy].balance = balanceThi Reference: https://github.com/crytic/slither/wiki/U</li> </ul>	iHarvest (contracts/BaseVault.sol#435) Detector—Documentation#reentrancy-vulnerabilities=1
BaseVaultorganizeWithdrawalQueue().offset (contr BaseVault.harvest(BaseStrategy[]).totalProfitAccru BaseVault.rebalance().amountsToInvest (contracts/Ba Reference: https://github.com/crytic/Slither/wiki/	acts/SaskVult.col2239) is a local variable nover initialized ad (contracts/SaskVult.col2458) is a local variable nover initialized aseVvult.sol2656) is a local variable nover initialized Detector-DocumentationAuninitialized-local-variables
	-590) ignoras raturn value by strategy-divast(currStrategyTVL – idealStrategyTVL) (contracts/BaseVault.sol#567) Datector-Documentation#unused-raturn
	dgeEscrow)governance (contracts/BaseVault.sol#37) lacks a zero-check on : tr/BaseVault.sol#2/)
<ul> <li>governance = _governance (contrac BaseVault.baseInitialize(address,ERC20,address,Brid wormboleRouter = wormboleRouter</li> </ul>	tty/BaseVault.sol842) dgeEscrow), worsholeRouter (contracts/BaseVault.sol837) lacks a zero-check on : (contracts/BaseVault.sol844)
BridgeEscrow.constructor(address), owner (contracts	s/BridgeEscrow.sol#28) lacks a zero-check on :
BridgeEscrow.initialize(address,IRootChainManager). - vault = _vault (contracts/Bridgef - wormholeDouter = BaseVault/comut	Exrom.slu29) wult (contracts/BridgeEscrow.sol#32) lacks a zero-check on : &erom.sol#015() (.wormAbJRAOUTE)( (contracts/BridgeEscrow.sol#36) Detector-Documentation#disising-zero-address-walidation
BaseVault.removeStrategy(BaseStrategy) (contracts/B	ulticall.sol#9-27) has external calls inside a loop: (success,result) = address(this).dologatecall(data[i]) (contracts/external/Multicall.sol#12) BareYault.sol#24-271) has external calls inside a loop: amountWithdrawm = strategy.dvest(typel)(uint250) maxi ( cult.col#47-452) has external calls inside a loop: BarenethisHarvest = strategy.dvest(typel)(uint250) has external calls inside a loop: BarenethisHarvest = strategy.dvest(typel)(uint250) has external/ABArValL.sol#242)
BaseVault.rebalance() (contracts/BaseVault.sol#549- BaseVault.rebalance() (contracts/BaseVault.sol#549-	uult-aol4407-442) has esterni calls inside a loop: bäinechnisHarvest = strateny-totallookkaValue() (ontracts/BaseVault-sol442) -590) has esterni calls inside a loop: anountToInvest = Math.min(amountToInvest, asset.balanceOf(address(this))) (contracts/BaseVault.sol4583) -590) has esterni calls inside a loop: strategy_scope_linvest(amountToInvest) (contracts/BaseVault.sol4588)
BaseVault.rebalance() (contracts/BaseVault.sol#549- BaseVault.rebalance() (contracts/BaseVault.sol#549- Reference: https://github.com/crytic/slither/wiki/[	-570) has external calls inside a loop: currStrategyTVL = strategy.totällockedValue() (contracts/BaseVault.sol#565) 190) has external calls inside a loop: strategy.divest(currStrategyTVL - idealStrategyTVL) (contracts/BaseVault.sol#567) Detector-Documentation/#calls-inside-a-loop
Reentrancy in BaseVault.removeStrategy(BaseStrategy External calls: - amountWithdrawn = strategy.divest(type())	(uint254).max) (contracts/BaseVault.sol#257)
State variables written after the call(s):	awa (aantyaata/Bacalault aal#947)
<ul> <li>totalStrategyHoldings -= oldBal (contract Reentrancy in BaseVault.withdrawFromStrategy(BaseSt External calls:</li> </ul>	mm (colicity/sistemic/solito/) KBaseValits(21259) trategy,uint266) (contracts/BaseVault.sol#362-376):
<ul> <li>amountWithdrawn = strategy.divest(tokenAm State variables written after the call(s):</li> </ul>	
<ul> <li>strategies[strategy].balance -= amountWit</li> <li>totalStrategyHoldings -= amountWithdrawn</li> <li>Reference: https://github.com/crvtic/slither/wiki/I</li> </ul>	bdfram (contracts/BaseWault.sol#366) (contracts/BaseWault.sol#371) Detector-Douenation#reentrancy-vulnerabilities-2
Reentrancy in BaseVault.depositIntoStrategy(BaseSt	
External calls: - strategy.invest(tokenAmount) (contracts/ Event emitted after the call(s):	
<ul> <li>StrategyDeposit(strategy,tokenAmount) (cr Reentrancy in BaseVault.withdrawFromStrategy(BaseS)</li> </ul>	ontracts/BaseVault.sol#338) trategy,uint256) (contracts/BaseVault.sol#362-376):
External calls: - amountWithdrawn = strategy.divest(tokenAm Event emitted after the call(s):	
<ul> <li>StrategyWithdrawal(strategy,amountWithdra</li> </ul>	awn) (contracts/BaseYault.scl8974) Detector-Documentation#reentrancy-vulnerabilities-3
BaseVault.harvest(BaseStrategy[]) (contracts/BaseVa Dangerous comparisons:	
- require(bool,string)(block.timestamp >= : BaseVault.lockedProfit() (contracts/BaseVault.sol#4	lastHarvest + lockInterval,PROFIT_UNLOCKING) (contracts/BaseVault.sol#409) 468-475) uses timestamp for comparisons
Dangerous comparisons: - block.timestamp >= lastHarvest + lockInte Reference: https://github.com/crytic/slither/wiki/k	erval (contracts/BaseVault.sol#669) Detector-Documentation#Djock-timestamp
Multicall.multicall(bytes[]) (contracts/external/M	ulticall.sol#9-27) uses assembly
<ul> <li>INLINE ASM (contracts/external/Multicall Reference: https://github.com/crytic/slither/wiki/K</li> </ul>	
BaseVault.removeStrategy(BaseStrategy) (contracts/ - totalBps -= stratInfo.tvlBps (contracts/i	BaseVault.solfX04-271) has costly operations inside a loop: BaseVault.solfX88) BaseVault.solfX40-271) has costly operations inside a loop:
Basevault.removeStrategy(BaseStrategy) (contracts/f — totalStrategyHoldings —= oldBal (contract BaseVault.removeStrategy(BaseStrategy) (contracts/f	masserunt, soizedezzz) mar costly operations inside a loop: ts/BaseYault.soiZeZeZz) has costly operations inside a loop: BaseYault.soiZeZeZzZ) has costly operations inside a loop:
<pre>- maxLockedProfit += oldBal - amountWithdr: BaseVault.updateStrategyAllocations(BaseStrategy[])</pre>	VERSENTENTENTENTENTENTENTENTENTENTENTENTENTE
	ult.sol200) Detector-Documentation#costly-operations-inside-s-loop
BaseVault_liquidate(uint256) (contracts/BaseVault BaseVault_depositIntoStrategies() (contracts/BaseV BaseVault_depositIntoStrategy(BaseStrategy, uint256 BaseVault_withdrawFromStrategy(BaseStrategy, uint256 WormholeRouter_validateWormholeMessageEmitter(TWo Reference: https://github.com/cytic/slitter/withs/	ault.sol#842-353) is newer used and should be removed (contracts/BaseYault.sol#825-370) is never used and should be removed a) (contracts/BaseYault.sol#826-376) is never used and should be removed rmole.WM) (contracts/Drambledouter.sol#41-50) is never used and should be removed
Pragma version^0.8.13 (contracts/AffineGovernable.	sol#2) necessitates a version too recent to be trusted. Consider deploving with 0.6.12/0.7.6/0.8.7
pragma version~0.8.13 (Contracts/BaseStrategy.sol#; Pragma version^0.8.13 (contracts/BaseVault.sol#2) : Pragma version^0.8.13 (contracts/BridgeEscrow.sol#;	2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/1.8.7 necessitates a version too recent to be trusted. Consider deploying mith 8.6.12/0.7.6/1.8.7 2) necessitates a version too recent to be trusted. Consider deploying with 8.6.12/0.7.6/1.8.7
Pragma version^0.8.13 (contracts/WormholeRouter.so. Pragma version^0.8.13 (contracts/external/Multical)	1#2) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7 1.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
Pragma version^0.8.13 (contracts/interfaces/IVault Pragma version^0.8.13 (contracts/interfaces/IWormh	hsinManger.sol42) nocessitates a version too recent to be trusted. Consider døploying with 4.6.12/4.7.6/0.8.7 .sol#2) nocessitates a version too recent to be trusted. Consider døploying with 4.6.12/0.7.6/0.8.7 Dis.sol#2) nocessitates a version too recent to be trusted. Consider døploying with 4.6.12/0.7.6/0.8.7
solc-0.8.16 is not recommended for deployment	Detector-Documentation#incorrect-versions-of-solidity
Low level call in Multicall.multicall(bytes[]) (cos - (success,result) = address(this).delegate	ntracts/external/Multicall.sol#9-27): meall(data(i)) (contracts/external/Multicall.sol#12)
	eall(dat(i)) (contract/strenz)/Multicall.sol#12) Detector-Documentationflow-level-cults Detector-Documentationflow-level-cults establishes and the second second second second second (second for the s
Reference: https://github.com/crytic/slither/wiki/l	256,uint256).newStrategy1 (contracts/BaseVault.sol#131) is too similar to BaseVault.swapWithdrawalQueueIndexes(uint256).newStrategy2 (contracts/BaseVault.so Detector-Documentation#variable-names-are-too-similar
BaseStrategy (contracts/BaseStrategy.sol#9-48) doe: - BaseStrategy.balanceOfAsset() (contracts, - BaseStrategy.divest(uint256) (contracts/	s not implement functions: //BaseStrategy.sol#250
<ul> <li>BaseStrategy.invest(uint256) (contracts/i BaseStrategy.totalLockedValue() (contract</li> </ul>	basestrategy.sol#x4) ts/BaseStrategy.sol#x4)
Reference: https://github.com/crytic/slither/wiki/f BridgeEscrow.vaultNonce (contracts/BridgeEscrow.so	Detector-Documentation#unimplemented-functions
WormholeRouter.nextValidNonce (contracts/WormholeRouter.otherLaverChainId (contracts/Wormho)	laRuter.sol#15) should be constant LaRuter.sol#15) should be constant
WormholeRouter.otherLayerRouter (contracts/Wormhole	eRoutes - solatal about de constant Distoito-Documant index de variable entret-cou id-be-declared-constant

AUTOMATED TESTING

 As a result of the tests carried out with the Slither tool, some results were obtained and reviewed by Halborn. Based on the results reviewed, some vulnerabilities were determined to be false positives. The actual vulnerabilities found by Slither are already included in the report findings.

# 4.2 AUTOMATED SECURITY SCAN

#### Description:

Halborn used automated security scanners to assist with detection of well-known security issues, and to identify low-hanging fruits on the targets for this engagement. Among the tools used was MythX, a security analysis service for Ethereum smart contracts. MythX performed a scan on all the contracts and sent the compiled results to the analyzers to locate any vulnerabilities.

#### MythX results:

<pre>src/ethereum/L1CompoundStrategy.sol</pre>					
Line	SWC Title	Severity	Short Description		
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.		
102	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
148	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
150	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "*" discovered		
150	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "/* discovered		
150	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
152	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
160	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
162	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
173	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
173	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
173	(SWC-101) Integer Overflow and Underflow	Unknown	Compiler-rewritable " <uint> - 1" discovered</uint>		
178	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
187	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
190	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
192	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
193	(SWC-110) Assert Violation	Unknown	Out of bounds array access		

#### src/ethereum/L1Vault.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

#### src/ethereum/L1WormholeRouter.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.
14	(SWC-108) State Variable Default Visibility	Low	State variable visibility is not set.

#### src/external/Multicall.sol

Line	SWC Title	Severity	Short Description
9	(SWC-118) Incorrect Constructor Name	Medium	Potential incorrect constructor name "multicall".
11	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "++" discovered
12	(SWC-110) Assert Violation	Unknown	Out of bounds array access
25	(SWC-110) Assert Violation	Unknown	Out of bounds array access

# src/polygon/EmergencyWithdrawalQueue.sol

		<u>, , , , , , , , , , , , , , , , , , , </u>		
Line	SWC Title		Severity	Short Description
2	(SWC-103)	Floating Pragma	Low	A floating pragma is set.
18	(SWC-108)	State Variable Default Visibility	Low	State variable visibility is not set.
61	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered
61	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered
71	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered
73	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered
74	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered
83	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-=" discovered
84	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-=" discovered
93	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered
99	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered
104	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered
105	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-=" discovered
115	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "++" discovered
118	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-=" discovered
119	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered

# src/polygon/ERC4626Router.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.
7	(SWC-123) Requirement Violation	Low	Requirement violation.
55	(SWC-123) Requirement Violation	Low	Requirement violation.

# src/polygon/ERC4626RouterBase.sol

Line	SWC Title	Severity	Short Description
1	(SWC-103) Floating Pragma	Low	A floating pragma is set.
41	(SWC-107) Reentrancy	Low	A call to a user-supplied address is executed.

# src/polygon/Forwarder.sol

Li	ne	SWC Title	Severity	Short Description
	2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

# src/polygon/L2AAVEStrategy.sol

Line	SWC Title		Severity	Short Description
2	(SWC-103)	Floating Pragma	Low	A floating pragma is set.
54	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered
54	(SWC-110)	Assert Violation	Unknown	Out of bounds array access
54	(SWC-101)	Integer Overflow and Underflow	Unknown	Compiler-rewritable " <uint> - 1" discovered</uint>
114	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered
156	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered
158	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered
158	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "/" discovered
158	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "*" discovered
160	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered
171	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "+* discovered
182	(SWC-101)	Integer Overflow and Underflow	Unknown	Compiler-rewritable " <uint> - 1" discovered</uint>
182	(SWC-110)	Assert Violation	Unknown	Out of bounds array access
182	(SWC-101)	Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered
187	(SWC-110)	Assert Violation	Unknown	Out of bounds array access
198	(SWC-110)	Assert Violation	Unknown	Out of bounds array access
201	(SWC-110)	Assert Violation	Unknown	Out of bounds array access
203	(SWC-110)	Assert Violation	Unknown	Out of bounds array access
284	(SWC-110)	Assert Violation	Unknown	Out of bounds array access

AUTOMATED TESTING

#### src/polygon/L2Vault.sol

Line         SNC Title         Severity         Short Description           2         (SNC-183) Floating Pragma         Low         A floating pragma is set.           44         (SNC-183) Integr everflow and Underflow         Unknown         Arithmatic operation *-1 discovered           44         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation *-1 discovered           46         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           47         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           48         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           49         (SNC-181) Assert Violation         Unknown         Arithmatic operation ** discovered           241         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           243         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           244         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           245         (SNC-181) Integr everflow and Underflow         Unknown         Arithmatic operation ** discovered           246         (SNC-		c/porygon/lzvddrt.sor				
64         SWC-181         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           64         SWC-181         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           64         SWC-181         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           67         SWC-181         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           68         SWC-183         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           188         SWC-183         Assert Violation         Unknown         Out of bounds array access           199         SWC-183         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           246         SWC-183         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           246         SWC-183         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           246         SWC-183         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           247         SWC-183         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discove	Line	SWC Title	Severity	Short Description		
46         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation '/' discovered           46         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation '/' discovered           47         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation '/' discovered           47         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation '/' discovered           48         [SWC-181] Assert Violation         Unknown         Out of bounds array access           294         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           244         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           246         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           246         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           246         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           246         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           241         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operat	2	(SWC-103) Floating Pragma	Low	A floating pragma is set.		
64         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           67         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           67         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           68         [SWC-181] Assert Violation         Unknown         Out of bounds array access           286         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           216         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           226         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           226         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           226         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           231         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           331         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           331         [SWC-181] Integer Overflow and Underflow         Unknown         Arithmetic operation	64	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
67       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation */ discovered         67       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         188       (SWC-181) Assert Violation       Unknown       Out of bounds array access         199       (SWC-181) Integer Overflow and Underflow       Unknown       Out of bounds array access         199       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         241       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         248       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         248       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         249       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         241       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         250       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         251       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         256       (SWC-181) Integer Overfl	66	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "/" discovered		
47       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         188       [SWC-181] Assert Violation       Unknown       Out of bounds array access         199       [SWC-181] Assert Violation       Unknown       Out of bounds array access         199       [SWC-181] Assert Violation       Unknown       Arithmetic operation ** discovered         216       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         214       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         226       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         226       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         237       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         238       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         239       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         249       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         247       [SWC-181] Integer Overflow and Underflow	66	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation *** discovered		
188         UNLOW         Out of bounds array access           199         [SWC-110] Assert Violation         Unknown         Out of bounds array access           225         [SWC-10] Assert Violation         Unknown         Arithmatic operation ** discovered           241         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           246         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           246         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           246         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           241         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           352         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           353         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           354         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           355         [SWC-10] Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           355         [SWC-10] Integer	67	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "/" discovered		
199       (SWC-10) Assert Violation       Unknown       Out of bounds sray access         225       (SWC-10) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         241       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         242       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         244       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         245       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         246       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         331       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         3351       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         346       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         355       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         356       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmatic operation ** discovered         357       (SWC-101) Intege	67	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "*" discovered		
225       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         241       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         248       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         248       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         246       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         312       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         311       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         313       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         316       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         316       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         317       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered         318       [SWC-181] Integer Overflow and Underflow       Unknown       Arithmetic operation *** discovered <td< td=""><td>108</td><td>(SWC-110) Assert Violation</td><td>Unknown</td><td>Out of bounds array access</td></td<>	108	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
241       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         268       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         264       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         264       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         266       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         351       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         351       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         354       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         355       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         365       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         373       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         374       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         374	109	(SWC-110) Assert Violation	Unknown	Out of bounds array access		
248         SWC-181         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           244         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           259         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           351         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           351         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           351         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           355         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           366         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           367         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           373         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           374         (SWC-181)         Integer Overflow and Underflow         Unknown </td <td>225</td> <td>(SWC-101) Integer Overflow and Underflow</td> <td>Unknown</td> <td>Arithmetic operation "+" discovered</td>	225	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
224         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           299         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           311         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation ** discovered           311         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           313         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           326         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           346         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           346         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           347         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           343         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           343         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmatic operation *- discovered           343         (SWC-181) Integer Overflow and Underflow         Unknown	241	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
298         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           312         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           331         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           331         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           331         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           341         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           354         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           359         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           453         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           453         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           454         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           454         (SWC-181) Integer Overflow and Underflow         Unknown	248	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
312       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         331       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         331       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         334       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         345       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         346       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         349       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         347       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         343       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         343       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         344       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         345       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation discovered         346	284	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
331         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           331         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           346         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           346         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           347         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           349         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           349         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           3473         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           3473         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           3474         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           3474         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           3474         (SWC-101) Integer Overflow and Underflow         Unknown	290	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
331         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           346         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           345         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           346         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           349         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           449         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           473         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           473         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           474         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           474         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           475         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           476         (SWC-101) Integer Overflow and Underflow         Unknown	312	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
345         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation '/ discovered           345         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation '* discovered           346         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           349         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           347         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           343         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           473         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           474         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           474         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           475         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           476         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           476         (SWC-181) Integer Overflow and Underflow         Unknown	331	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
365         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation *** discovered           399         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation *** discovered           469         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation *** discovered           473         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           473         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           473         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           474         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           474         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           475         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           476         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           476         [SWC-101] Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           476         [SWC-101] Integer Overflow and Underflow         Unknown	331	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
399       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         449       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         474       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         474       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         477       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         478       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         478       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         474	345	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "/" discovered		
449       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         474       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         476       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         477       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         478       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514	365	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "*" discovered		
473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         473       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         473       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         474       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         474       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         584       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514	399	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation '/ discovered         473       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation '* discovered         474       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         474       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         476       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         477       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         580       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514       (SWC-101) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         514	469	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
473       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation ** discovered         474       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         476       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         477       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         560       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         514       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         528       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         522	473	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
4/4       (SWC-183) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         4/6       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         4/6       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         4/7       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/8       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/4       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/4       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/4       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/4       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/4       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/8       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/8       (SWC-181) Integer Overflow and Underflow       Unknown       Arithmetic operation *- discovered         5/8	473	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "/" discovered		
446         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           447         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           549         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           544         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           524         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           528         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           522         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered	473	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "*" discovered		
497         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           599         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           520         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           522         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered	474	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
569         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           528         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           522         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered	496	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation *- discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation */ discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           526         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           526         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           522         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered	497	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
514         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation */* discovered           514         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-181)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           528         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered           522         (SWC-101)         Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered	509	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
514         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           514         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation ** discovered           528         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered           529         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered           522         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered	514	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
514         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *+* discovered           528         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered           522         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered           529         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered	514	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "/" discovered		
528         (SWC-181) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered           522         (SWC-101) Integer Overflow and Underflow         Unknown         Arithmetic operation *-* discovered	514	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "*" discovered		
522 (SWC-101) Integer Overflow and Underflow Unknown Arithmetic operation "-" discovered	514	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered		
	520	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
	522	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "-" discovered		
549 (SWC-101) Integer Overflow and Underflow Unknown Arithmetic operation "+=" discovered	549	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+=" discovered		

# src/polygon/L2WormholeRouter.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.
14	(SWC-108) State Variable Default Visibility	Low	State variable visibility is not set.
51	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered
64	(SWC-101) Integer Overflow and Underflow	Unknown	Arithmetic operation "+" discovered

src/AffineGovernable.sol

#### src/BaseStrategy.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

### src/BaseVault.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.
31	(SWC-108) State Variable Default Visibility	Low	State variable visibility is not set.

#### src/BridgeEscrow.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

#### src/Constants.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

#### src/DollarMath.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

# src/WormholeRouter.sol

Line	SWC Title	Severity	Short Description
2	(SWC-103) Floating Pragma	Low	A floating pragma is set.

• No major issues found by Mythx. The floating pragma flagged by MythX is a false positive, as the pragma is set in the hardhat.config.ts file to the 0.8.16 version.



THANK YOU FOR CHOOSING