MythX

REPORT 5F5A66D3909C42001948C3A1

Created	Thu Sep 10 2020 17:48:03 GMT+0000 (Coordinated Universal Time)
Number of analyses	15
User	jameskey@protonmail.com

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
6d136d81-3c5c-4ab6-8023-018a9e7bfe17	contracts/rsv-v2/Manager.sol	0
4f674fc8-fff6-4412-bbaa-30fb553b9dfd	contracts/rsv-v2/Proposal.sol	1
2e4a10ff-fa2f-4fd1-ae08-93e14d69792c	contracts/rsv-v2/zeppelin/GSN/Context.sol	0
abbf381b-18bb-42ea-ba65-9924c2976192	contracts/rsv-v2/Proposal.sol	1
18f0c721-31a5-41fd-8666-cf709c0ceb1e	contracts/rsv-v2/ownership/OwnableV2.sol	0
397cc488-03d0-4149-9874-deeb03e7fded	contracts/rsv-v2/rsv/ReserveEternalStorage.sol	0
22f87bf8-0ecf-4c78-86de-6b5f4ca6ae9f	contracts/rsv-v2/rsv/Reserve.sol	0
97a53544-bb59-4c96-bf94-76cf84bb16ba	contracts/rsv-v2/Proposal.sol	2
f297d832-3505-4af9-a6b6-359a90098dd7	contracts/rsv-v2/Vault.sol	2
4768e9cf-c800-4198-988c-56b1e9dc28c2	contracts/rsv-v2/zeppelin/token/ERC20/ERC20V2.sol	0
6decc491-205f-47d4-af15-3da148d3f3b1	contracts/rsv-v2/rsv/Relayer.sol	0
acb102e1-3a08-4f16-9b87-50227fa25bff	contracts/rsv-v2/Basket.sol	2
c764cdd4-771a-471c-a4d5-3ec92753b507	contracts/rsv-v2/LockerFactory.sol	0
91c18476-641f-4d32-9957-715becf748f2	contracts/rsv-v2/Proposal.sol	1
73e21402-98de-4c33-bd28-e3a1b8b61afc	contracts/rsv-v2/Locker.sol	3

Analysis 6d136d81-3c5c-4ab6-8023-018a9e7bfe17

MythX

Started	Thu Sep 10 2020 17:48:15 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:03:26 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	Contracts/Rsv-V2/Manager.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis 4f674fc8-fff6-4412-bbaa-30fb553b9dfd

MythX

Started	Thu Sep 10 2020 17:48:15 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:04:06 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Proposal.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	1

ISSUES

LOW

SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

`contracts/rsv-v2/zeppelin/math/SafeMathV2.sol`

Locations

```
pragma solidity 0.5.7;

/**
```

Analysis `2e4a10ff-fa2f-4fd1-ae08-93e14d69792c` MythX

Started	
Finished	Thu Sep 10 2020 17:48:14 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Zeppelin/GSN/Context.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis abbf381b-18bb-42ea-ba65-9924c2976192 MythX

Started	Thu Sep 10 2020 17:48:25 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 17:48:27 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	Contracts/Rsv-V2/Proposal.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	1

ISSUES

LOW

SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

contracts/rsv-v2/zeppelin/token/ERC20/SafeERC20V2.sol

Locations

```
pragma solidity 0.5.7;

import "./IERC20.sol";
```

Analysis `18f0c721-31a5-41fd-8666-cf709c0ceb1e` MythX

Started	
Finished	Thu Sep 10 2020 17:48:19 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Ownership/OwnableV2.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis 397cc488-03d0-4149-9874-deeb03e7fded MythX

Started	Thu Sep 10 2020 17:48:25 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:03:36 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Rsv/ReserveEternalStorage.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis 22f87bf8-0ecf-4c78-86de-6b5f4ca6ae9f

MythX

Started	Thu Sep 10 2020 17:48:25 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:04:12 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Rsv/Reserve.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis 97a53544-bb59-4c96-bf94-76cf84bb16ba MythX

Started	Thu Sep 10 2020 17:48:35 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:03:50 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	Contracts/Rsv-V2/Proposal.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	2

ISSUES

LOW SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

contracts/rsv-v2/zeppelin/token/ERC20/SafeERC20V2.sol

Locations

```
pragma solidity 0.5.7;

import "./IERC20.sol";
```

Analysis `f297d832-3505-4af9-a6b6-359a90098dd7` MythX

Started	Thu Sep 10 2020 17:48:35 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:03:46 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Vault.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	2

ISSUES

LOW

SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

`contracts/rsv-v2/zeppelin/utils/AddressV2.sol`

Locations

```

pragma solidity 0.5.7;

/**
```

LOW

SWC-123

Requirement violation.

A requirement was violated in a nested call and the call was reverted as a result. Make sure valid inputs are provided to the nested call (for instance, via passed arguments).

Source file

`contracts/rsv-v2/zeppelin/utils/AddressV2.sol`

Locations

```
*
* This test is non-exhaustive, and there may be false-negatives: during the
* execution of a contract's constructor, its address will be reported as
* not containing a contract.
*
* IMPORTANT: It is unsafe to assume that an address for which this
* function returns false is an externally-owned account (EOA) and not a
* contract.
*/
function isContract(address account) internal view returns (bool) {
// This method relies in extcodesize, which returns 0 for contracts in
// construction, since the code is only stored at the end of the
// constructor execution.

// According to EIP-1052, 0x0 is the value returned for not-yet created accounts
// and 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470 is returned
// for accounts without code, i.e. `keccak256('')`
bytes32 codehash;
bytes32 accountHash = 0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470;
// solhint-disable-next-line no-inline-assembly
assembly { codehash := extcodehash(account) }
return (codehash != 0x0 && codehash != accountHash);
}

/**
* @dev Converts an `address` into `address payable`. Note that this is
* simply a type cast: the actual underlying value is not changed.
*
* NOTE: This is a feature of the next version of OpenZeppelin Contracts.
* @dev Get it via `npm install @openzeppelin/contracts@next`.
*/
```

Analysis `4768e9cf-c800-4198-988c-56b1e9dc28c2` MythX

Started	Thu Sep 10 2020 17:48:35 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:03:46 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Zeppelin/Token/ERC20/ERC20V2.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis 6decc491-205f-47d4-af15-3da148d3f3b1 MythX

Started	
Finished	Thu Sep 10 2020 17:48:36 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	Contracts/Rsv-V2/Rsv/Relayer.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis acb102e1-3a08-4f16-9b87-50227fa25bff

MythX

Started	
Finished	Thu Sep 10 2020 17:48:39 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/Basket.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	2

ISSUES

LOW SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

`contracts/rsv-v2/Basket.sol`

Locations

```
pragma solidity 0.5.7;

```

LOW SWC-128

Implicit loop over unbounded data structure.

Gas consumption in function "getTokens" in contract "Basket" depends on the size of data structures that may grow unboundedly. The highlighted statement involves copying the array "tokens" from "storage" to "memory". When copying arrays from "storage" to "memory" the Solidity compiler emits an implicit loop.If the array grows too large, the gas required to execute the code will exceed the block gas limit, effectively causing a denial-of-service condition. Consider that an attacker might attempt to cause this condition on purpose.

Source file

`contracts/rsv-v2/Basket.sol`

Locations

```

function getTokens() external view returns(address[] memory) {
return tokens;
}
```

Analysis `c764cdd4-771a-471c-a4d5-3ec92753b507` MythX

Started	Thu Sep 10 2020 17:48:46 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:03:58 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	`Contracts/Rsv-V2/LockerFactory.Sol`

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

Analysis 91c18476-641f-4d32-9957-715becf748f2

MythX

Started	Thu Sep 10 2020 17:48:56 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 17:49:04 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	Contracts/Rsv-V2/Proposal.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	1

ISSUES

LOW

SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

contracts/rsv-v2/zeppelin/math/SafeMathV2.sol

Locations

```
pragma solidity 0.5.7;

/**
```

Analysis 73e21402-98de-4c33-bd28-e3a1b8b61afc MythX

Started	Thu Sep 10 2020 17:48:56 GMT+0000 (Coordinated Universal Time)
Finished	Thu Sep 10 2020 18:04:06 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Brownie-1.11.0
Main Source File	Contracts/Rsv-V2/Locker.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	3

ISSUES

LOW

SWC-102

An outdated compiler version is used.

The compiler version specified in the pragma directive may have known bugs. It is recommended to use the latest minor release of solc 0.5 or 0.6. For more information on Solidity compiler bug reports and fixes refer to https://github.com/ethereum/solidity/releases.

Source file

contracts/rsv-v2/zeppelin/math/SafeMathV2.sol

Locations

```
pragma solidity 0.5.7;

/**
```

LOW

SWC-116

A control flow decision is made based on The block.timestamp environment variable.

The block.timestamp environment variable is used to determine a control flow decision. Note that the values of variables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicious miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment variables as sources of randomness and be aware that use of these variables introduces a certain level of trust into miners.

Source file

contracts/rsv-v2/zeppelin/math/SafeMathV2.sol

Locations

```
*
* Requirements:
* - Subtraction cannot overflow.
*/
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
return sub(a, b, "SafeMath: subtraction overflow");
}
```

LOW

SWC-116

A control flow decision is made based on The block.timestamp environment variable.

The block.timestamp environment variable is used to determine a control flow decision. Note that the values of variables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicious miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment variables as sources of randomness and be aware that use of these variables introduces a certain level of trust into miners.

Source file

`contracts/rsv-v2/zeppelin/math/SafeMathV2.sol`

Locations

```
*
* Requirements:
* - Subtraction cannot overflow.
*/
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
return sub(a, b, "SafeMath: subtraction overflow");
}
```