

REPORT 642314174CD3DD001AC13977

Created	Tue Mar 28 2023 16:21:43 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	60be4a3d43f2c340d312dbe0

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
00e6a2c8-2b85-44e2-a9e9-52bc03bf7074	Bribe.sol	0

Started	Tue Mar 28 2023 16:21:53 GMT+0000 (Coordinated Universal Time)
Finished	Tue Mar 28 2023 16:22:00 GMT+0000 (Coordinated Universal Time)
Mode	Deep
Client Tool	Remythx
Main Source File	Bribe.sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	0

ISSUES

UNKNOWN Arithmetic operation "+" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file
SafeERC20.sol
Locations

```
38 | token,  
39 | abi.encodeWithSelector(token.transferFrom.selector, from, to, value)  
40 |  
41 |  
42 |  
43 | function safeApprove(  
44 | IERC20 token,  
45 | address spender,  
46 | uint256 value
```

UNKNOWN Arithmetic operation "+" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
38 | token,  
39 | abi.encodeWithSelector(token.transferFrom.selector, from, to, value)  
40 |  
41 |  
42 |  
43 | function safeApprove() function safeApprove(  
44 | IERC20 token,  
45 | address spender,
```

UNKNOWN Arithmetic operation "/" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
38 | token,  
39 | abi.encodeWithSelector(token.transferFrom.selector, from, to, value)  
40 | );  
41 | }
```

UNKNOWN Arithmetic operation "/" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
39 | abi.encodeWithSelector(token.transferFrom.selector, from, to, value)  
40 | );  
41 |  
42 |  
43 | function safeApprove(  
44 | IERC20 token,
```

UNKNOWN Arithmetic operation "/" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
41 | }  
42 |  
43 | function safeApprove(  
44 |     IERC20 token,  
45 |     address spender,  
46 |     uint256 value
```

UNKNOWN Arithmetic operation "+" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
41 | }  
42 |  
43 | function safeApprove(  
44 |     IERC20 token,  
45 |     address spender,
```

UNKNOWN Arithmetic operation "%" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
41 | }  
42 |  
43 | function safeApprove(  
44 |     IERC20 token,  
45 |     address spender,
```

UNKNOWN Arithmetic operation "%" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

SafeERC20.sol

Locations

```
41 | }  
42 |  
43 | function safeApprove(  
44 | IERC20 token,  
45 | address spender,
```

UNKNOWN Arithmetic operation "+" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

Address.sol

Locations

```
48 | function isContract(address account) internal view returns (bool) {  
49 | // This method relies on extcodesize/address.code.length, which returns 0  
50 | // for contracts in construction, since the code is only stored at the end  
51 | // of the constructor execution.  
52 |  
53 | return account.code.length > 0;
```

UNKNOWN Arithmetic operation "-" discovered

This plugin produces issues to support false positive discovery within MythX.

SWC-101

Source file

Address.sol

Locations

```
59 | *  
60 | * https://eips.ethereum.org/EIPS/eip-1884[EIP1884] increases the gas cost  
61 | * of certain opcodes, possibly making contracts go over the 2300 gas limit  
62 | * imposed by 'transfer', making them unable to receive funds via  
63 | * 'transfer'. {sendValue} removes this limitation.  
64 | *
```

UNKNOWN Public state variable with array type causing reachable exception by default.

The public state variable "rewardTokens" in "Bribe" contract has type "address[]" and can cause an exception in case of use of invalid array index value.

SWC-110

Source file

IProtocolGovernance.sol

Locations

```
35 function voter() external view returns (address);
36
37 function stableMiner() external view returns (address);
38
39 function baseReferralsContract() external view returns (address);
40
41 function baseReferralFee() external view returns (uint256);
```