MythX

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
0e0f2b5b-153e-4c6e-af44-56e51583ab0e	TimestampValidator.sol	2
89918838-6071-484a-838d-65e10cdd9227	loyaltySettings.sol	2
133a593c-26f3-465d-a63b-22eb744d1440	SparkleToken.sol	1

Started	Wed Aug 26 2020 01:41:23 GMT+0000 (Coordinated Universal Time)
Finished	Wed Aug 26 2020 01:56:36 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Mythx-Cli-0.6.19
Main Source File	TimestampValidator.Sol

DETECTED VULNERABILITIES

(HIGH   (MEDIUM   (LOW

1   0   1

ISSUES

HIGH

SWC-101

The arithmetic operator can overflow.

It is possible to cause an integer overflow or underflow in the arithmetic operation.

Source file

TimestampValidator.sol

Locations

```
43   uint256 currentTime = block.timestamp;
44   uint256 depositTime = block.timestamp;
45   uint256 rewardTime = block.timestamp + verifyTimeLegnth;
46   require (verifyTimeLegnth == 60, 'timestamps do not match');
47   require (currentTime == block.timestamp, 'timestamps do not match');
```

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An outdated compiler version is used.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

TimestampValidator.sol

Locations

```
1   pragma solidity 0.4.25;
2
3   import './ReentrancyGuard.sol';
```

Started	Wed Aug 26 2020 01:41:23 GMT+0000 (Coordinated Universal Time)
Finished	Wed Aug 26 2020 01:56:55 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Mythx-Cli-0.6.19
Main Source File	LoyaltySettings.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An outdated compiler version is used.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
loyaltySettings.sol
Locations

```
1  pragma solidity 0.4.25;
2
```

LOW

SWC-113

Multiple calls are executed in the same transaction.

This call is executed following another call within the same transaction. It is possible that the call never gets executed if a prior call fails permanently. This might be caused intentionally by a malicious callee. If possible, refactor the code such that each transaction only executes one external call or make sure that all callees can be trusted (i.e. they're part of your own codebase).

Source file
loyaltySettings.sol
Locations

```
257  POL._rewardTime = POL._depositTime.add(_timeLegnth);
258  time.setTimestamp(msg.sender);
259  token.transferFrom(address(msg.sender), address(this), _value);
260  } else {
261  revert ('Unexspected error ');
```

Started	Wed Aug 26 2020 01:41:33 GMT+0000 (Coordinated Universal Time)
Finished	Wed Aug 26 2020 01:56:44 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Client Tool	Mythx-Cli-0.6.19
Main Source File	SparkleToken.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
SparkleToken.sol
Locations

```
3    */
4
5    pragma solidity 0.4.25;
6
7    // File: openzeppelin-solidity/contracts/token/ERC20/IERC20.sol
```