

REPORT 5FBAC7171E71B80019020492

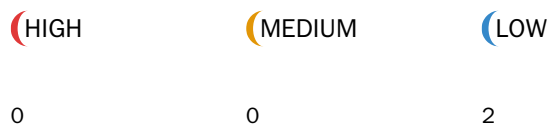
Created Sun Nov 22 2020 20:16:23 GMT+0000 (Coordinated Universal Time)
Number of analyses 1
User shailendrakumarmkar@gmail.com

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
4e1e1057-eeff-4a2c-9d65-f3635c2579bf	/contracts/marketplace.sol	2

Started	Sun Nov 22 2020 20:16:25 GMT+0000 (Coordinated Universal Time)
Finished	Sun Nov 22 2020 20:18:31 GMT+0000 (Coordinated Universal Time)
Mode	Quick
Client Tool	Mythx-Vscode-Extension
Main Source File	/Contracts/Marketplace.Sol

DETECTED VULNERABILITIES



ISSUES

- LOW** An outdated compiler version is used.
- SWC-102** 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/marketplace.sol

Locations

```
1 | pragma solidity 0.5.0;
2 |
3 | /// @title Marketplace
```

- LOW** Call with hardcoded gas amount.
- SWC-134** The highlighted function call forwards a fixed amount of gas. This is discouraged as the gas cost of EVM instructions may change in the future, which could break this contract's assumptions. If this was done to prevent reentrancy attacks, consider alternative methods such as the checks-effects-interactions pattern or reentrancy locks instead.

Source file
/contracts/marketplace.sol

Locations

```
92 | products[_id] = _product;
93 |
94 | address(seller).transfer(msg.value);
95 |
96 | emit ProductPurchased(_id,_product.name,_product.price,msg.sender,true);
```