MythX

REPORT 655F572F5E6443001A5930E0

Created	Thu Nov 23 2023 13:44:15 GMT+0000 (Coordinated Universal Time)
Number of analyses	1
User	637bc5fd8288ab39b9a0547b

REPORT SUMMARY

Analyses ID	Main source file	Detected vulnerabilities
6d19bb3b-2e74-404f-a5fc-278968811788	CryptoPesos.sol	67

Analysis 6d19bb3b-2e74-404f-a5fc-278968811788 MythX

Started	Thu Nov 23 2023 13:44:25 GMT+0000 (Coordinated Universal Time)
Finished	Thu Nov 23 2023 13:44:41 GMT+0000 (Coordinated Universal Time)
Mode	Quick
Client Tool	Remythx
Main Source File	CryptoPesos.Sol

DETECTED VULNERABILITIES

HIGH	MEDIUM	LOW
0	0	67

ISSUES

UNKNOWN Arithmetic operation "+=" discovered

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

SWC-101

Source file
CryptoPesos.sol
Locations

```
599 if (from == address(0)) {
600 // Overflow check required: The rest of the code assumes that totalSupply never overflows
601 _totalSupply += value;
602 } else {
603 uint256 fromBalance = _balances[from];
604 if (fromBalance < value) {
```

UNKNOWN Arithmetic operation "-" discovered

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

SWC-101

Source file
CryptoPesos.sol
Locations

```
607 unchecked {
608 // Overflow not possible: value <= fromBalance <= totalSupply.
609 _balances[from] = fromBalance - value;
610 }
611 }
```

UNKNOWN

Arithmetic operation "-=" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
614 | unchecked {
615 | // Overflow not possible: value <= totalSupply or value <= fromBalance <= totalSupply.
616 | _totalSupply -= value;
617 | }
618 | } else {
619 | unchecked {
```

UNKNOWN

Arithmetic operation "+=" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
619 | unchecked {
620 | // Overflow not possible: balance + value is at most totalSupply, which we know fits into a uint256.
621 | _balances[to] += value;
622 | }
623 | }
```

UNKNOWN

Arithmetic operation "-" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
720 | }
721 | unchecked {
722 | _approve(owner, spender, currentAllowance - value, false);
723 | }
724 | }
```

UNKNOWN

Arithmetic operation "++" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
989 address pair = FACTORY.createPair(address(this), ROUTER.WETH());
990 pancakeSwapPair[pair] = true;
991 for (uint i = 0; i < tokenFees.length; i++) {
992 pair = FACTORY.createPair(address(this), tokenFees[i]);
993 pancakeSwapPair[pair] = true;
994 }
```

UNKNOWN

Arithmetic operation "/" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
1017 if (isPair(sender)) {
1018 //It's an LP Pair and it's a buy
1019 taxAmount = (amount * buyTax) / PERCENT_DIVIDER;
1020 } else if (isPair(receiver)) {
1021 //It's an LP Pair and it's a sell
1022 taxAmount = (amount * sellTax) / PERCENT_DIVIDER;
```

UNKNOWN

Arithmetic operation "*" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
1017 if (isPair(sender)) {
1018 //It's an LP Pair and it's a buy
1019 taxAmount = (amount * buyTax) / PERCENT_DIVIDER;
1020 } else if (isPair(receiver)) {
1021 //It's an LP Pair and it's a sell
```

UNKNOWN Arithmetic operation "/" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
1020 } else if (isPair(receiver)) {
1021 //It's an LP Pair and it's a sell
1022 taxAmount = (amount * sellTax) / PERCENT_DIVIDER;
1023 }
1024 }
```

UNKNOWN Arithmetic operation "*" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
1020 } else if (isPair(receiver)) {
1021 //It's an LP Pair and it's a sell
1022 taxAmount = (amount * sellTax) / PERCENT_DIVIDER;
1023 }
1024 }
```

UNKNOWN Arithmetic operation "/" discovered

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

SWC-101

Source file

CryptoPesos.sol

Locations

```
1025
1026 if (taxAmount > 0) {
1027 uint _toDev = taxAmount / devFeeDivider;
1028 super._update(sender, devWallet, _toDev);
1029 super._update(sender, ownerWallet, taxAmount - _toDev);
1030 }
```

UNKNOWN

SWC-101

Arithmetic operation "-" discovered

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

Source file

CryptoPesos.sol

Locations

```
1027 uint _toDev = taxAmount / devFeeDivider;
1028 super._update(sender, devWallet, _toDev);
1029 super._update(sender, ownerWallet, taxAmount - _toDev);
1030 }
1031 super._update(sender, receiver, amount - taxAmount);
1032 }
```

UNKNOWN

SWC-101

Arithmetic operation "-" discovered

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

Source file

CryptoPesos.sol

Locations

```
1029 super._update(sender, ownerWallet, taxAmount - _toDev);
1030 }
1031 super._update(sender, receiver, amount - taxAmount);
1032 }
1033
1034 fallback() external {
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
8  // OpenZeppelin Contracts (last updated v5.0.0) (utils/Context.sol)
9
10 pragma solidity ^0.8.20;
11
12 /**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
36 // OpenZeppelin Contracts (last updated v5.0.0) (access/Ownable.sol)
37
38 pragma solidity ^0.8.20;
39
40 /**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
137 // Original license: SPDX_License_Identifier: MIT
138 // OpenZeppelin Contracts (last updated v5.0.0) (interfaces/draft-IERC6093.sol)
139 pragma solidity ^0.8.20;
140
141 /**
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
303 // OpenZeppelin Contracts (last updated v5.0.0) (token/ERC20/IERC20.sol)
304
305 pragma solidity ^0.8.20;
306
307 /**
308 * @dev Interface of the ERC20 standard as defined in the EIP. * @dev Interface of the ERC20 standard as defined in the EIP.
309 */
310 interface IERC20 {
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
386 // OpenZeppelin Contracts (last updated v5.0.0) (token/ERC20/extensions/IERC20Metadata.sol)
387
388 pragma solidity ^0.8.20;
389
390 /**
391 * @dev Interface for the optional metadata functions from the ERC20 standard. * @dev Interface for the optional metadata functions from the ERC20 standard.
392 */
393 interface IERC20Metadata is IERC20 {
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
414 // OpenZeppelin Contracts (last updated v5.0.0) (token/ERC20/ERC20.sol)
415
416 pragma solidity ^0.8.20;
417
418
419
420
421 /**
422 * @dev Implementation of the {IERC20} interface.
423 *
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
730
731 // Original license: SPDX_License_Identifier: MIT
732 pragma solidity ^0.8.20;
733
734 interface IUniswapV2Router01 {
735 function factory() external pure returns (address);
736 function WETH() external pure returns (address);
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""^0.8.20"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
830
831 // Original license: SPDX_License_Identifier: MIT
832 pragma solidity ^0.8.20;
833
834 interface IUniswapV2Router02 is IUniswapV2Router01 {
835 function removeLiquidityETHSupportingFeeOnTransferTokens(
836 address token,
```

LOW

SWC-103

A floating pragma is set.

The current pragma Solidity directive is ""=0.5.0"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source file

CryptoPesos.sol

Locations

```
877
878 // Original license: SPDX_License_Identifier: MIT
879 pragma solidity >=0.5.0;
880
881 interface IUniswapV2Factory {
882 event PairCreated(address indexed token0, address indexed token1, address pair, uint);
```

LOW

SWC-108

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "OwnableUnauthorizedAccount" is internal. Other possible visibility settings are public and private.

Source file

CryptoPesos.sol

Locations

```
56 * @dev The caller account is not authorized to perform an operation.
57 */
58 error OwnableUnauthorizedAccount(address account);
59
60 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "account" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
56  * @dev The caller account is not authorized to perform an operation.
57  */
58  error OwnableUnauthorizedAccount(address account);
59
60  /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "OwnableInvalidOwner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
61  * @dev The owner is not a valid owner account. (eg. `address(0)`)
62  */
63  error OwnableInvalidOwner(address owner);
64
65  event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "owner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
61  * @dev The owner is not a valid owner account. (eg. `address(0)`)
62  */
63  error OwnableInvalidOwner(address owner);
64
65  event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC20InsufficientBalance" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
150 * @param needed Minimum amount required to perform a transfer.
151 */
152 error ERC20InsufficientBalance(address sender, uint256 balance, uint256 needed);
153
154 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "sender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
150 * @param needed Minimum amount required to perform a transfer.
151 */
152 error ERC20InsufficientBalance(address sender, uint256 balance, uint256 needed);
153
154 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "balance" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
150 * @param needed Minimum amount required to perform a transfer.
151 */
152 error ERC20InsufficientBalance(address sender, uint256 balance, uint256 needed);
153
154 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "needed" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
150 * @param needed Minimum amount required to perform a transfer.
151 */
152 error ERC20InsufficientBalance(address sender, uint256 balance, uint256 needed);
153
154 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC20InvalidSender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
156 * @param sender Address whose tokens are being transferred.
157 */
158 error ERC20InvalidSender(address sender);
159
160 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "sender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
156 * @param sender Address whose tokens are being transferred.
157 */
158 error ERC20InvalidSender(address sender);
159
160 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC20InvalidReceiver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
162 * @param receiver Address to which tokens are being transferred.
163 */
164 error ERC20InvalidReceiver(address receiver);
165
166 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "receiver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
162 * @param receiver Address to which tokens are being transferred.
163 */
164 error ERC20InvalidReceiver(address receiver);
165
166 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC20InsufficientAllowance" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
170 * @param needed Minimum amount required to perform a transfer.
171 */
172 error ERC20InsufficientAllowance(address spender, uint256 allowance, uint256 needed);
173
174 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "spender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
170 * @param needed Minimum amount required to perform a transfer.
171 */
172 error ERC20InsufficientAllowance(address spender, uint256 allowance, uint256 needed);
173
174 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "allowance" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
170 * @param needed Minimum amount required to perform a transfer.
171 */
172 error ERC20InsufficientAllowance(address spender, uint256 allowance, uint256 needed);
173
174 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "needed" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
170 * @param needed Minimum amount required to perform a transfer.
171 */
172 error ERC20InsufficientAllowance(address spender, uint256 allowance, uint256 needed);
173
174 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC20InvalidApprover" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
176 * @param approver Address initiating an approval operation.
177 */
178 error ERC20InvalidApprover(address approver);
179
180 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "approver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
176 * @param approver Address initiating an approval operation.
177 */
178 error ERC20InvalidApprover(address approver);
179
180 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC20InvalidSpender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
182 * @param spender Address that may be allowed to operate on tokens without being their owner.
183 */
184 error ERC20InvalidSpender(address spender);
185 }
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "spender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
182 * @param spender Address that may be allowed to operate on tokens without being their owner.
183 */
184 error ERC20InvalidSpender(address spender);
185 }
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721InvalidOwner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
195 * @param owner Address of the current owner of a token.
196 */
197 error ERC721InvalidOwner(address owner);
198
199 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "owner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
195 * @param owner Address of the current owner of a token.
196 */
197 error ERC721InvalidOwner(address owner);
198
199 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721NonexistentToken" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
201 * @param tokenId Identifier number of a token.
202 */
203 error ERC721NonexistentToken(uint256 tokenId);
204
205 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "tokenId" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
201 * @param tokenId Identifier number of a token.
202 */
203 error ERC721NonexistentToken(uint256 tokenId);
204
205 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721IncorrectOwner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
209 * @param owner Address of the current owner of a token.
210 */
211 error ERC721IncorrectOwner(address sender, uint256 tokenId, address owner);
212
213 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "sender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
209 * @param owner Address of the current owner of a token.
210 */
211 error ERC721IncorrectOwner(address sender, uint256 tokenId, address owner);
212
213 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "tokenId" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
209 * @param owner Address of the current owner of a token.
210 */
211 error ERC721IncorrectOwner(address sender, uint256 tokenId, address owner);
212
213 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "owner" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
209 * @param owner Address of the current owner of a token.
210 */
211 error ERC721IncorrectOwner(address sender, uint256 tokenId, address owner);
212
213 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721InvalidSender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
215 * @param sender Address whose tokens are being transferred.
216 */
217 error ERC721InvalidSender(address sender);
218
219 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "sender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
215 * @param sender Address whose tokens are being transferred.
216 */
217 error ERC721InvalidSender(address sender);
218
219 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721InvalidReceiver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
221 * @param receiver Address to which tokens are being transferred.
222 */
223 error ERC721InvalidReceiver(address receiver);
224
225 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "receiver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
221 * @param receiver Address to which tokens are being transferred.
222 */
223 error ERC721InvalidReceiver(address receiver);
224
225 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721InsufficientApproval" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
228 * @param tokenId Identifier number of a token.
229 */
230 error ERC721InsufficientApproval(address operator, uint256 tokenId);
231
232 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "operator" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
228 * @param tokenId Identifier number of a token.
229 */
230 error ERC721InsufficientApproval(address operator, uint256 tokenId);
231
232 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "tokenId" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
228 * @param tokenId Identifier number of a token.
229 */
230 error ERC721InsufficientApproval(address operator, uint256 tokenId);
231
232 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721InvalidApprover" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
234 * @param approver Address initiating an approval operation.
235 */
236 error ERC721InvalidApprover(address approver);
237
238 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "approver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
234 * @param approver Address initiating an approval operation.
235 */
236 error ERC721InvalidApprover(address approver);
237
238 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC721InvalidOperator" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
240 * @param operator Address that may be allowed to operate on tokens without being their owner.
241 */
242 error ERC721InvalidOperator(address operator);
243 }
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "operator" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
240 * @param operator Address that may be allowed to operate on tokens without being their owner.
241 */
242 error ERC721InvalidOperator(address operator);
243 }
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155InsufficientBalance" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
255 * @param tokenId Identifier number of a token.
256 */
257 error ERC1155InsufficientBalance(address sender, uint256 balance, uint256 needed, uint256 tokenId);
258
259 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "sender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
255 * @param tokenId Identifier number of a token.
256 */
257 error ERC1155InsufficientBalance(address sender, uint256 balance, uint256 needed, uint256 tokenId);
258
259 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "balance" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
255 * @param tokenId Identifier number of a token.
256 */
257 error ERC1155InsufficientBalance(address sender, uint256 balance, uint256 needed, uint256 tokenId);
258
259 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "needed" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
255 * @param tokenId Identifier number of a token.
256 */
257 error ERC1155InsufficientBalance(address sender, uint256 balance, uint256 needed, uint256 tokenId);
258
259 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "tokenId" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
255 * @param tokenId Identifier number of a token.
256 */
257 error ERC1155InsufficientBalance(address sender, uint256 balance, uint256 needed, uint256 tokenId);
258
259 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155InvalidSender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
261 * @param sender Address whose tokens are being transferred.
262 */
263 error ERC1155InvalidSender(address sender);
264
265 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "sender" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
261 * @param sender Address whose tokens are being transferred.
262 */
263 error ERC1155InvalidSender(address sender);
264
265 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155InvalidReceiver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
267 * @param receiver Address to which tokens are being transferred.
268 */
269 error ERC1155InvalidReceiver(address receiver);
270
271 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "receiver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
267 * @param receiver Address to which tokens are being transferred.
268 */
269 error ERC1155InvalidReceiver(address receiver);
270
271 /**
```

LOW

SWC-108

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155MissingApprovalForAll" is internal. Other possible visibility settings are public and private.

Source file

CryptoPesos.sol

Locations

```
274 * @param owner Address of the current owner of a token.
275 */
276 error ERC1155MissingApprovalForAll(address operator, address owner);
277
278 /**
```

LOW

SWC-108

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "operator" is internal. Other possible visibility settings are public and private.

Source file

CryptoPesos.sol

Locations

```
274 * @param owner Address of the current owner of a token.
275 */
276 error ERC1155MissingApprovalForAll(address operator, address owner);
277
278 /**
```

LOW

SWC-108

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "owner" is internal. Other possible visibility settings are public and private.

Source file

CryptoPesos.sol

Locations

```
274 * @param owner Address of the current owner of a token.
275 */
276 error ERC1155MissingApprovalForAll(address operator, address owner);
277
278 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155InvalidApprover" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
280 * @param approver Address initiating an approval operation.
281 */
282 error ERC1155InvalidApprover(address approver);
283
284 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "approver" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
280 * @param approver Address initiating an approval operation.
281 */
282 error ERC1155InvalidApprover(address approver);
283
284 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155InvalidOperator" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
286 * @param operator Address that may be allowed to operate on tokens without being their owner.
287 */
288 error ERC1155InvalidOperator(address operator);
289
290 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "operator" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
286 * @param operator Address that may be allowed to operate on tokens without being their owner.
287 */
288 error ERC1155InvalidOperator(address operator);
289
290 /**
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "ERC1155InvalidArrayLength" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
294 * @param valuesLength Length of the array of token amounts
295 */
296 error ERC1155InvalidArrayLength(uint256 idsLength, uint256 valuesLength);
297 }
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "idsLength" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
294 * @param valuesLength Length of the array of token amounts
295 */
296 error ERC1155InvalidArrayLength(uint256 idsLength, uint256 valuesLength);
297 }
```

LOW

State variable visibility is not set.

It is best practice to set the visibility of state variables explicitly. The default visibility for "valuesLength" is internal. Other possible visibility settings are public and private.

SWC-108

Source file

CryptoPesos.sol

Locations

```
294 * @param valuesLength Length of the array of token amounts
295 */
296 error ERC1155InvalidArrayLength(uint256 idsLength, uint256 valuesLength);
297 }
```

UNKNOWN Out of bounds array access

The index access expression can cause an exception in case of use of invalid array index value.

SWC-110

Source file

CryptoPesos.sol

Locations

```
990 pancakeSwapPair[pair] = true;
991 for (uint i = 0; i < tokenFees.length; i++) {
992 pair = FACTORY.createPair(address(this), tokenFees[i]);
993 pancakeSwapPair[pair] = true;
994 }
995 }
```