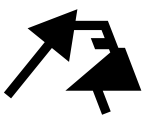
Flype Maximaizer Audit Report

Dec 03, 2022



WATCHPUG

Table of Contents

Summary

This report has been prepared for Flype Maximaizer Audit Report smart contract, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Overview

Project Summary

Project Name	**Flype Maximaizer Audit Report**
Codebase	**https://github.com/Flype-organization/maximaizer**
Commit	**edf8b6a3eeda3edc315b3e96b60689b792ead1b4**
Language	**Solidity**

Audit Summary

Delivery Date	**Dec 03, 2022**
Audit Methodology	**Static Analysis, Manual Review**
Total Isssues	**3**

[WP-S1] `restrictedMintToggle` can be changed to `bool`

Issue Description

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/FlypeMaxiVaultV1.sol#L86-L152

```
86      function mint(uint256 mintAmount, address receiver)
87          external
88          nonReentrant
89          returns (
90              uint256 amount0,
91              uint256 amount1,
92              uint128 liquidityMinted
93          )
94      {
95          require(mintAmount > 0, "mint 0");
96          require(
97              restrictedMintToggle != 11111 || msg.sender == _manager,
98              "restricted"
99          );
100
    @@ 101,151 @@
152     }
```

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/abstract/FlypeMaxiVaultV1Storage.sol#L146-L152

```
146     function toggleRestrictMint() external onlyManager {
147         if (restrictedMintToggle == RESTRICTED_MINT_ENABLED) {
148             restrictedMintToggle = 0;
149         } else {
150             restrictedMintToggle = RESTRICTED_MINT_ENABLED;
151         }
152     }
```

https://github.com/Flype-organization/maximaizer/blob/

edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/abstract/FlypeMaxiVaultV1Storage.sol#L27-L29

```
27      /// @dev "restricted mint enabled" toggle value must be a number
28      // above 10000 to safely avoid collisions for repurposed state var
29      uint16 public constant RESTRICTED_MINT_ENABLED = 11111;
```

Using `11111` instead of `true` for `restrictedMintToggle` is an inferior choice for backward compatibility reasons.

Changing it to a `bool` is preferred for better readability.

Status

✓ Fixed

[WP-N2] Wrong Comment

Issue Description

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/vendor/proxy/EIP173Proxy.sol#L87-L95

```
87      // returns the proxy admin address from the memory slot using assembly
88      function _proxyAdmin() internal view returns (address adminAddress) {
89          // solhint-disable-next-line security/no-inline-assembly
90          assembly {
91              adminAddress := sload(
92                  0xb53127684a568b3173ae13b9f8a6016e243e63b6e8ee1178d6a717850b5d6103
93              )
94          }
95      }
```

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/vendor/proxy/Proxy.sol#L53-L90

```
53      function _setImplementation(address newImplementation, bytes memory data)
54          internal
55      {
56          // retrive the previousImplementation address from the memory slot
57          address previousImplementation;
58          // solhint-disable-next-line security/no-inline-assembly
59          assembly {
60              previousImplementation := sload(
61                  0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc
62              )
63          }
64
65          // the newImplementation address in the memory slot
66          // solhint-disable-next-line security/no-inline-assembly
67          assembly {
68              sstore(
69
    0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc,
70                  newImplementation
```

```
71              )
72          }
73
    @@ 74,89 @@
90      }
```

`memory slot` should be `storage slot` .

Recommendation

Consider changing to:

```
87      // returns the proxy admin address from the storage slot using assembly
88      function _proxyAdmin() internal view returns (address adminAddress) {
89          // solhint-disable-next-line security/no-inline-assembly
90          assembly {
91              adminAddress := sload(
92                  0xb53127684a568b3173ae13b9f8a6016e243e63b6e8ee1178d6a717850b5d6103
93              )
94          }
95      }
```

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/vendor/proxy/Proxy.sol#L53-L90

```
53      function _setImplementation(address newImplementation, bytes memory data)
54          internal
55      {
56          // retrive the previousImplementation address from the storage slot
57          address previousImplementation;
58          // solhint-disable-next-line security/no-inline-assembly
59          assembly {
60              previousImplementation := sload(
61                  0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc
62              )
63          }
64
65          // the newImplementation address in the storage slot
```

```
66          // solhint-disable-next-line security/no-inline-assembly
67          assembly {
68              sstore(
69
    0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc,
70                  newImplementation
71              )
72          }
73
    @@ 74,89 @@
90      }
```

Status

✓ Fixed

[WP-I3] Typo

Informational

Issue Description

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/abstract/FlypeMaxiFactoryV1Storage.sol#L21

```
21  address public vaultmplementation;
```

https://github.com/Flype-organization/maximaizer/blob/edf8b6a3eeda3edc315b3e96b60689b792ead1b4/contracts/FlypeMaxiFactoryV1.sol#L141-L158

```
141 function upgradeVaults(address[] memory vaults) external onlyManager {
142     for (uint256 i = 0; i < vaults.length; i++) {
143         IEIP173Proxy(vaults[i]).upgradeTo(vaultmplementation);
144     }
145 }
146
147 function upgradeVaultsAndCall(
148     address[] memory vaults,
149     bytes[] calldata datas
150 ) external onlyManager {
151     require(vaults.length == datas.length, "mismatching array length");
152     for (uint256 i = 0; i < vaults.length; i++) {
153         IEIP173Proxy(vaults[i]).upgradeToAndCall(
154             vaultmplementation,
155             datas[i]
156         );
157     }
158 }
```

`vaultmplementation` -> `vaultImplementation`

Status

✓ Fixed

Appendix

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by WatchPug; however, WatchPug does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Smart Contract technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.