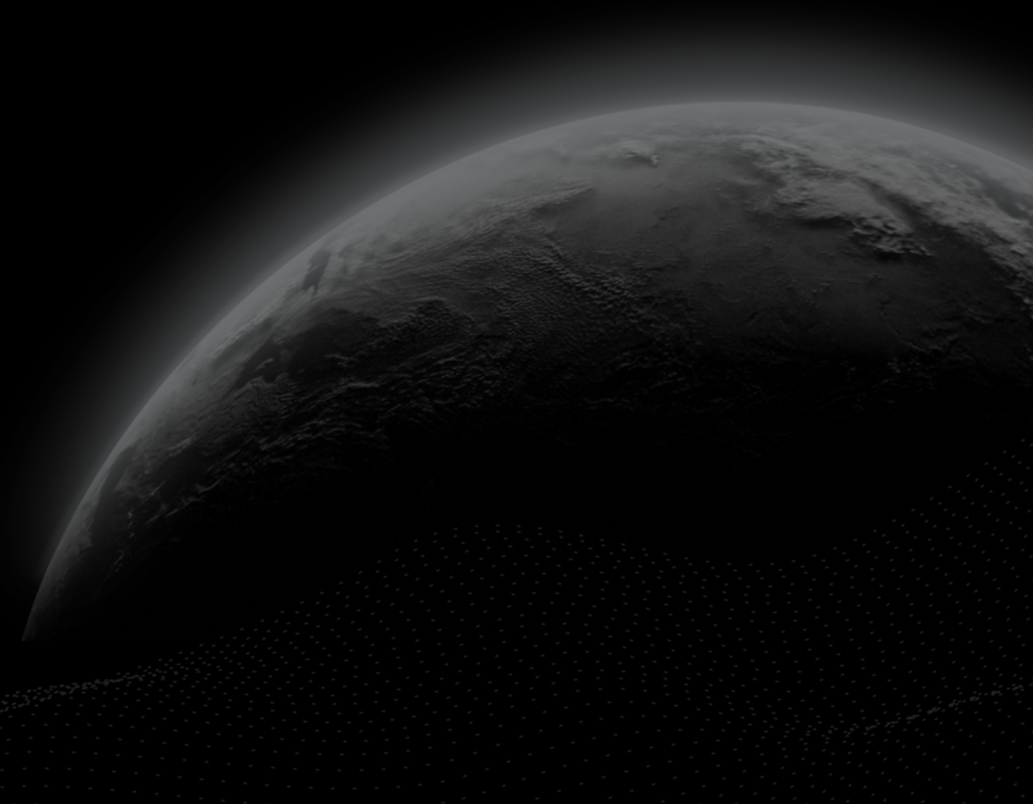
Security Assessment

ManifoldXYZ

CertiK Verified on Mar 22nd, 2023



CertiK Verified on Mar 22nd, 2023

ManifoldXYZ

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
NFT	Ethereum (ETH)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 03/22/2023	N/A

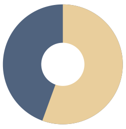
CODEBASE

update 75dcb6e40ce933e72c0cd7d4ddd5af1edc0e5cda

base 17505a3f1a75b0ecb979339a5296f596416180f3

...View All

Vulnerability Summary



9	8	0	0	1	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

■	0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
■	0	Major		Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
■	0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
■	5	Minor	4 Resolved, 1 Acknowledged	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
■	4	Informational	4 Resolved	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | MANIFOLDXYZ

CODEBASE | MANIFOLDXYZ

Repository

update 75dcb6e40ce933e72c0cd7d4ddd5af1edc0e5cda

base 17505a3f1a75b0ecb979339a5296f596416180f3

AUDIT SCOPE | MANIFOLDXYZ

56 files audited ● 1 file with Acknowledged findings ● 14 files with Resolved findings ● 41 files without findings

ID	File	SHA256 Checksum
● RCC	contracts/ERC1155Creator.sol	1fbdd74211afb0d79a6000b78dda5590a4a53a3ae08c0800cd6c3f1c2e49fba5
● CCB	contracts/core/CreatorCore.sol	99a6b8cf0dea2204477b32d10114ffe63bb13acc7c90d97626762ceadd5241e8
● ERC	contracts/core/ERC1155CreatorCore.sol	e39131128e7ea92f734abeb7a1fb0a7104ec6e32fa1e1377b0794553ee44d0b9
● ECC	contracts/core/ERC721CreatorCore.sol	b37bc1bdfd836ddbc7bb9596bca6d6ba53bd08d9140aa588beb00836f10ea0ac
● ERE	contracts/core/ERC721CreatorCoreEnumerable.sol	7e5c7f9b4ba6fb8b10604ada68168b367bf0020461186e5ba4fd8180abd1eaab
● ERB	contracts/extensions/ERC1155/ERC1155CreatorExtensionBurnable.sol	710facc4ded9054a52682eccb3f86d872a306deca61b85d29f246131afd7d1ba
● ECE	contracts/extensions/ERC721/ERC721CreatorExtensionBurnable.sol	64b16bce4500ff771ef78d183e4a2eff86543c1afa9d90857968d1f911b529e1
● ERM	contracts/permissions/ERC1155/ERC1155CreatorMintPermissions.sol	f430252e1d286db39fe02cd6a5758aac10bf21570a075f7f19191bc05a42c5cb
● ERP	contracts/permissions/ERC721/ERC721CreatorMintPermissions.sol	fee8981ffe3cc890f53d27e540d40b2873b07f4b0a1b97549f341945c2c74a7e
● ECB	contracts/token/ERC1155/ERC1155Base.sol	0f606a06e69fb71bb278914d8da7d013d0ba2993a18ce2b8cd62d9bb47946ed8
● ERU	contracts/token/ERC1155/ERC1155Upgradeable.sol	d9f6bebf273d8040a065cfa6a460f58813f91221dd56a01991d08c126a38a178
● EER	contracts/token/ERC721/ERC721Core.sol	89413455984446100d234cfaf05b9fd39599e13a404fc9df74c7e2207accde5e
● EEE	contracts/token/ERC721/ERC721Enumerable.sol	c931f43d720b5060b16d7aa6faa219379a0caa3af4c3e72b9fc8f5beab3d5355
● ECU	contracts/token/ERC721/ERC721Upgradeable.sol	bb93aa72958cea26947e2dd37b551de7774709c862a4d9fb8c0b19bd47b81ce9

ID	File	SHA256 Checksum
● ERO	contracts/ERC721Creator.sol	65ce01b356ecc25a92ffc774b3b325fae66c7f60643f3fb36ced0b29a378fa8b
● ERA	contracts/extensions/ERC1155/ERC1155CreatorExtensionApproveTransfer.sol	1649243d68dd7c7b053c2e014a7b864b6ba5f1d52fbbcd39ce494829f3e38b21
● ERR	contracts/extensions/ERC721/ERC721CreatorExtension.sol	60828858bfddb1e6bd5275f325a7ee970196121a5e977ffa0b1f5d66dbcba516
● ERT	contracts/extensions/ERC721/ERC721CreatorExtensionApproveTransfer.sol	2c5809aa5b93e07160df00cbdb471923af66a18b0e1e1770bd511fa5604e3142
● CEB	contracts/extensions/CreatorExtension.sol	6caacf3f1f276dc906e2d496ba748e1e746707ccd3b4fe440441097bd6d260b6
● CRE	contracts/extensions/CreatorExtensionBasic.sol	d05162449070365c933180924cefe0482dd3a2313112ec29bc56e29691122bd8
● CER	contracts/extensions/CreatorExtensionRoyalties.sol	b5443ed0778e023adbbd7fbdd9c7872114ba7d6db195b372767adb9f4f0fd2ab
● ECR	contracts/token/ERC1155/ERC1155Core.sol	528cf00881c4b61f9884f64745e7d318684863ad12e96f31552a222c04caf616
● EBE	contracts/token/ERC721/ERC721Base.sol	82b903edb549bf802959852fbaefbfc4ef050d2ce1052fb36fe66a6a9dd6f51f
● ERI	contracts/ERC1155CreatorImplementation.sol	c5a1f12e16714f562271dc3b99aaf5a33949729f4693650e596845cfa561b5f4
● RCU	contracts/ERC1155CreatorUpgradeable.sol	536b75bb6214518ef1fa1c6e80138182ddccd60a345b34212ffa8c7645d79d28
● RCE	contracts/ERC721CreatorEnumerable.sol	d3d4024689f0d77008c5bb09e109ee871e0cce4e175cf895222427097c464423
● ECI	contracts/ERC721CreatorImplementation.sol	cc22bf18499c07a87ba65e5677a9e392b6feadd95f860b494697f6019349714d
● CCU	contracts/ERC721CreatorUpgradeable.sol	8c888099c0ea862520ba85188f92a22738be8e173f17f3cefa999b1da241370e
● CCH	contracts/core/CreatorCore.sol	68b156fad82dcc5114440e73b326330a3d7116d89222868e8506b20f8853d9a1
● CCC	contracts/core/ERC1155CreatorCore.sol	6ca281c077d62e3390e68f1682b3c311ef6ad0f78a925db7e4ff514aced54042
● ERN	contracts/core/ERC721CreatorCore.sol	c1c87705893fb216fe56c2a3681aca814d8b6a2a19b76e54f7507bd187a9a4be

ID	File	SHA256 Checksum
● CCE	contracts/core/ERC721CreatorCoreEnumerable.sol	bb8d59ffb238cbbc2443d75abdf812b838e118165e2223515f37c18f22f01534
● CEU	contracts/extensions/CreatorExtension.sol	6caacf3f1f276dc906e2d496ba748e1e746707ccd3b4fe440441097bd6d260b6
● CRA	contracts/extensions/CreatorExtensionBasic.sol	d05162449070365c933180924cefe0482dd3a2313112ec29bc56e29691122bd8
● CRT	contracts/extensions/CreatorExtensionRoyalties.sol	b5443ed0778e023adbbd7fbdd9c7872114ba7d6db195b372767adb9f4f0fd2ab
● ECA	contracts/extensions/ERC1155/ERC1155CreatorExtensionApproveTransfer.sol	1649243d68dd7c7b053c2e014a7b864b6ba5f1d52fbbcd39ce494829f3e38b21
● EEB	contracts/extensions/ERC1155/ERC1155CreatorExtensionBurnable.sol	7efeac75f3cc1233137b34b2808e9c36ea7f98e51bff17568f75fcb6b833d212
● EEC	contracts/extensions/ERC721/ERC721CreatorExtension.sol	60828858bfddb1e6bd5275f325a7ee970196121a5e977ffa0b1f5d66dbcba516
● ECT	contracts/extensions/ERC721/ERC721CreatorExtensionApproveTransfer.sol	2c5809aa5b93e07160df00cbdb471923af66a18b0e1e1770bd511fa5604e3142
● EBR	contracts/extensions/ERC721/ERC721CreatorExtensionBurnable.sol	b5596c9e86ef265ff6e37f7e9a853ca32ba5e5eaa52b3f8e5f509d4dc0ef3741
● ECM	contracts/permissions/ERC1155/ERC1155CreatorMintPermissions.sol	e924b6396f352e54b43051679ec485ba2dc17a49aa0f360cf59b1285ffd519b8
● ECP	contracts/permissions/ERC721/ERC721CreatorMintPermissions.sol	56cc5c3c986f70eed23120fe0afc5885ab4f9f9f581e4d9ed5a4836b1bbe0623
● EBC	contracts/token/ERC1155/ERC1155Base.sol	9e8289a80e0c7dfa8f1cec6cc593066f3079ca522c16922ef4edf9ff594a5ac8
● EUE	contracts/token/ERC1155/ERC1155Upgradeable.sol	f2ad7218b3668d3c1bfb80b87d5792f4637231e1b04b1b075e9bb08439f5f1d9
● RCR	contracts/token/ERC1155/ERC1155Core.sol	528cf00881c4b61f9884f64745e7d318684863ad12e96f31552a222c04caf616
● RCB	contracts/token/ERC721/ERC721Base.sol	82b903edb549bf802959852fbaefbfc4ef050d2ce1052fb36fe66a6a9dd6f51f
● RER	contracts/token/ERC721/ERC721Core.sol	1cb72203232a85dc4ba07517d16c039369db2d69be1f3a48293dbeded30fa85f

ID	File	SHA256 Checksum
● REE	contracts/token/ERC721/ERC721Enumerable.sol	3a7e085e4ed4f23f5ceb01afa3c21f5b782462d7c09eafc86ad6d94c3ad41730
● EUR	contracts/token/ERC721/ERC721Upgradeable.sol	f58ae18d07835a6df4a1bdf0f782d91d83c3e4445ec4e4fc042d53de1c84550e
● ERD	contracts/ERC1155Creator.sol	0c836fe91aa7347e7769130020c3a2d3ac416915066855abc195ffe2fe71a1a0
● RCI	contracts/ERC1155CreatorImplementation.sol	2da0c3c4dd4ccf2cdde10538cf0c19c58bd89a1ad3c05f189af6fe47924efd33
● ERG	contracts/ERC1155CreatorUpgradeable.sol	dabac36df8eb20b69600315230c2a67dc19892d6873e79c68eae5ff57b7b860c
● ER6	contracts/ERC721Creator.sol	93074abc021c21a9555e2b1b986f5b2262559dcc26db9e3573c71057579dd1d4
● CCI	contracts/ERC721CreatorImplementation.sol	8295f4063c59f58bd90f61a309f558c73e5271316c8940b6d6c9e664d1dda0b9
● ERL	contracts/ERC721CreatorUpgradeable.sol	79ff77ebe3b2e84d5281e5695933a159b60cfa781418318256959e6324ef7a36
● ER4	contracts/ERC721CreatorEnumerable.sol	d3d4024689f0d77008c5bb09e109ee871e0cce4e175cf895222427097c464423

APPROACH & METHODS | MANIFOLDXYZ

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

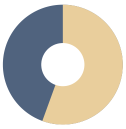
The auditing process pays special attention to the following considerations:

- 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.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

FINDINGS | MANIFOLDXYZ



9	0	0	0	5	4
Total Findings	Critical	Major	Medium	Minor	Informational

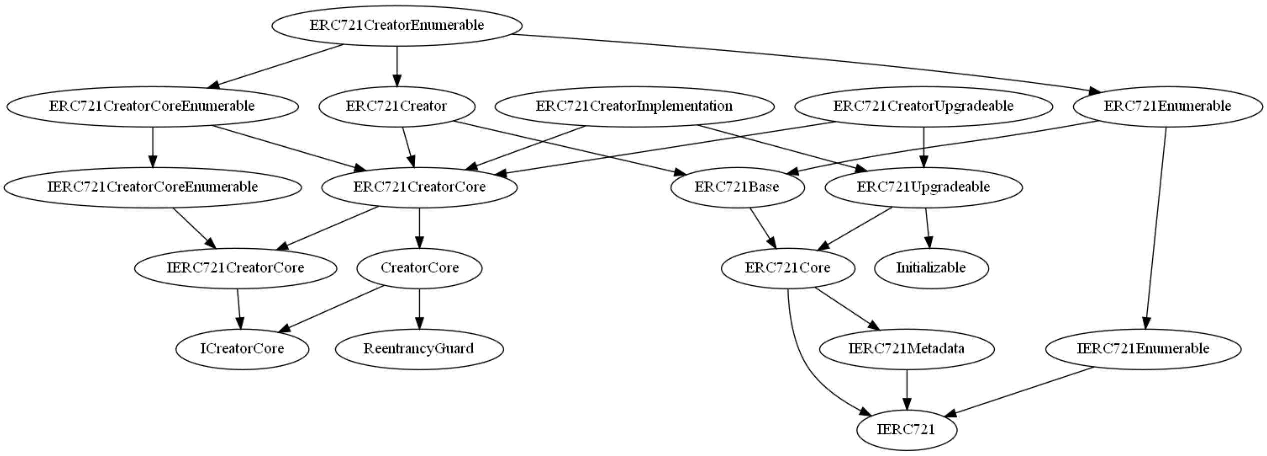
This report has been prepared to discover issues and vulnerabilities for ManifoldXYZ. Through this audit, we have uncovered 9 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
CCB-01	Inheritance Graph Is Overcomplicated	Coding Style	Minor	● Resolved
COR-01	Ambiguous Comment Of `_checkMintPermissions()`	Inconsistency	Minor	● Resolved
ECC-01	Potential Overflow Of `_extensionCounter`	Volatile Code	Minor	● Resolved
RCC-01	Lack Of Sanity Check In `_mintNew()`	Volatile Code	Minor	● Acknowledged
TOK-01	`__gap` Size Is Meaningless	Inconsistency	Minor	● Resolved
CON-01	Incorrect Comments	Coding Style	Informational	● Resolved
CON-02	Unused Functionality	Inconsistency	Informational	● Resolved
EER-01	Misleading Argument Name `extensionIndex`	Coding Style	Informational	● Resolved
ERE-01	`ERC721CreatorCoreEnumerable._beforeTokenTransfer()` Can Be Simplified	Coding Style	Informational	● Resolved

CCB-01 | INHERITANCE GRAPH IS OVERCOMPLICATED

Category	Severity	Location	Status
Coding Style	● Minor	contracts/core/CreatorCore.sol (base): 35~37	● Resolved

Description



The inheritance graph is overcomplicated and can be reworked. In particular:

1. `_extensionPermissions` and `_extensionApproveTransfers` are declared in `CreatorCore` but used only in `ERC721CreatorCore` and `ERC1155CreatorCore`.
2. `ERC721CreatorImplementation` and `ERC721CreatorUpgradeable` have identical implementations. `ERC1155CreatorImplementation` and `ERC1155CreatorUpgradeable` have identical implementations. The goal is unclear.

Recommendation

We recommend simplifying the inheritance graph.

Alleviation

[**Project team**]: `ERC721Implementation` is intended to be deployed once per chain and referenced by proxy contracts as an implementation reference. This allows us to deploy custom smart contracts (in that, there can be customized ascii) in a cheap manner.

COR-01 | AMBIGUOUS COMMENT OF `_checkMintPermissions()`

Category	Severity	Location	Status
Inconsistency	● Minor	contracts/core/ERC1155CreatorCore.sol (base): 57~58; contracts/core/ERC721CreatorCore.sol (base): 61~63	● Resolved

Description

```
61         * Check if an extension can mint
62         */
63       function _checkMintPermissions(address to, uint256 tokenId) internal {
```

The comment states that the function is supposed to check if an extension can mint. However, the actual logic is:

1. If the token admin didn't `setMintPermissions()` for a specific `extension`, then this extension can mint without restrictions.
2. If the token admin did `setMintPermissions(extension, permissions)`, then this `extension` can mint only if `approveMint()` call to `permissions` contract doesn't revert.

It is not documented if an `extension` is supposed to mint by default and can be restricted, or is supposed only mint if the permissions are set.

Recommendation

We recommend changing the comment to express the intended behavior in a more clear way.

ECC-01 | POTENTIAL OVERFLOW OF `_extensionCounter`

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/core/ERC721CreatorCore.sol (base): 129~130	● Resolved

Description

`ERC721CreatorCore` supposes there will be no more than 65535 extensions. However, it is not enforced by `_registerExtension()` .

Recommendation

We recommend adding an explicit check

```
require(_extensionCounter < uint16(-1), "Too many extensions");
```

RCC-01 | LACK OF SANITY CHECK IN `_mintNew()`

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/ERC1155Creator.sol (base): 196~197	● Acknowledged

Description

There is no check in `ERC1155Creator._mintNew()` that `to.length >= 1`. Empty array can be passed.

Recommendation

We recommend explicitly checking the size of `to`.

TOK-01 | `__gap` SIZE IS MEANINGLESS

Category	Severity	Location	Status
Inconsistency	● Minor	contracts/token/ERC1155/ERC1155Upgradeable.sol (base): 30~31; contracts/token/ERC721/ERC721Upgradeable.sol (base): 30~31	● Resolved

Description

```
30      uint256[44] private __gap;
```

`abstract` contract `ERC721Upgradeable` has `__gap` field with size 44. The contract doesn't occupy any storage slots itself. Parent `ERC721Core` occupies 6 storage slots but doesn't completely implement `IERC721Metadata`. `Initializable` also occupies some storage not accounted for by the `__gap`.

Contract inherited from `Initializable` should ensure the implementation contract can't be initialized:

```
/// @custom:oz-upgrades-unsafe-allow constructor
constructor() {
    _disableInitializers();
}
```

`abstract` contract `ERC1155Upgradeable` also has `__gap` field with size 44. However, parent `ERC1155Core` occupies only 4 storage slots.

`ERC1155CreatorUpgradeable` and `ERC721CreatorUpgradeable` don't have `__gap`, so can't be inherited in an upgradable way.

Recommendation

We recommend removing the `__gap` for `abstract` classes. We recommend preventing the implementation contract from being initialized.

CON-01 | INCORRECT COMMENTS

Category	Severity	Location	Status
Coding Style	● Informational	contracts/ERC1155Creator.sol (base): 361~362; contracts/ERC721Creator.sol (base): 299~300; contracts/core/ERC721CreatorCore.sol (base): 76~77; contracts/core/ERC721CreatorCoreEnumerable.sol (base): 94~95; contracts/extensions/ERC1155/ERC1155CreatorExtensionBurnable.sol (base): 47~48; contracts/extensions/ERC721/ERC721CreatorExtensionBurnable.sol (base): 77~78; contracts/permissions/ERC1155/ERC1155CreatorMintPermissions.sol (base): 34~35; contracts/permissions/ERC721/ERC721CreatorMintPermissions.sol (base): 34~35; contracts/token/ERC1155/ERC1155Base.sol (base): 8~9; contracts/token/ERC1155/ERC1155Upgradeable.sol (base): 9~10; contracts/token/ERC721/ERC721Core.sol (base): 413~414; contracts/token/ERC721/ERC721Enumerable.sol (base): 2~3	● Resolved

Description

```
76        * Override for post mint actions
```

The comment for `_preMintExtension()` doesn't reflect the function's meaning. In fact, `_preMintExtension()` is called pre-mint by `_mintExtension()`.

```
94        * @dev See {IERC721CeratorCoreEnumerable-tokenOfOwnerByIndeBase}.
```

`tokenOfOwnerByIndeBase` is supposed to be `tokenOfOwnerByIndexBase`.

```
77        * @dev See {IERC721CreatorExtension-onBurn}.
```

`IERC721CreatorExtension` is supposed to be `IERC721CreatorExtensionBurnable`.

```
34        * @dev See {IERC721CreatorMintPermissions-approve}.
```

`approve` is supposed to be `approveMint`.

```
2  // OpenZeppelin Contracts v4.4.1 (token/ERC721/extensions/ERC721Enumerable.sol)
```

The original contract was modified. The comment should be removed.

```
      * - `batchSize` is non-zero.
```

There is no `batchSize` argument in `_beforeTokenTransfer()` / `_afterTokenTransfer()` .

```
  * @dev Implementation of https://eips.ethereum.org/EIPS/eip-721[ERC721] Non-Fungible Token Standard
```

The comment in `ERC1155Base.sol` and `ERC1155Upgradable.sol` is supposed to be about ERC1155.

```
       * @dev See {IERC721CreatorCore-tokenExtension}.
```

`IERC721CreatorCore` is supposed to be `ICreatorCore` .

```
      * @dev See {IERC1155-uri}.
```

`IERC1155` is supposed to be `IERC1155MetadataURI` .

Recommendation

We recommend updating the comments.

CON-02 | UNUSED FUNCTIONALITY

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/core/ERC721CreatorCoreEnumerable.sol (base): 16~18; contracts/token/ERC721/ERC721Core.sol (base): 17~18	● Resolved

Description

```
16      using Strings for uint256;
17      using EnumerableSet for EnumerableSet.AddressSet;
```

`ERC721CreatorCoreEnumerable` doesn't use `Strings` and `EnumerableSet` .

Recommendation

We recommend removing of unused functionality.

EER-01 | MISLEADING ARGUMENT NAME `extensionIndex`

Category	Severity	Location	Status
Coding Style	● Informational	contracts/token/ERC721/ERC721Core.sol (base): 221	● Resolved

Description

```
221      function _safeMint(address to, uint256 tokenId, uint96 extensionIndex)
internal virtual {
```

`extensionIndex` argument is in fact `tokenData`, and index occupies only 16 bits.

Recommendation

We recommend renaming the argument to `tokenData` to better reflect the argument meaning.

ERE-01 `ERC721CreatorCoreEnumerable._beforeTokenTransfer()` CAN BE SIMPLIFIED

Category	Severity	Location	Status
Coding Style	● Informational	contracts/core/ERC721CreatorCoreEnumerable.sol (base): 130~139	● Resolved

Description

```
130          if (from != address(0) && to != address(0)) {
131              address tokenExtension_ = _indexToExtension[uint16(data)];
132              if (from != to) {
133                  _removeTokenFromOwnerEnumeration(from, tokenId,
tokenExtension_);
134              }
135              if (to != from) {
136                  _addTokenToOwnerEnumeration(to, tokenId, tokenExtension_);
137              }
138          }
139      }
```

Three `if` conditions can be merged into one.

Recommendation

We recommend rewriting the code this way:

```
130          if (from != address(0) && to != address(0) && from != to) {
131              address tokenExtension_ = _indexToExtension[uint16(data)];
132              _removeTokenFromOwnerEnumeration(from, tokenId, tokenExtension_);
133              _addTokenToOwnerEnumeration(to, tokenId, tokenExtension_);
134          }
135      }
```

OPTIMIZATIONS | MANIFOLDXYZ

ID	Title	Category	Severity	Status
CON-03	`memory` Argument Can Be Declared `calldata`	Gas Optimization	Optimization	● Resolved

CON-03 | `memory` ARGUMENT CAN BE DECLARED `calldata`

Category	Severity	Location	Status
Gas Optimization	● Optimization	contracts/ERC1155Creator.sol (base): 99~100, 132~133, 190~191, 247~248; contracts/ERC721Creator.sol (base): 96~97, 129~130; contracts/core/CreatorCore.sol (base): 208~209; contracts/core/ERC1155CreatorCore.sol (base): 59~60, 68~69, 86~87	● Resolved

Description

One or more parameters with `memory` data location are never modified in their functions and those functions are never called internally within the contract. Thus, their data location can be changed to `calldata` to avoid gas consumption copying from `calldata` to `memory` .

Recommendation

We recommend changing the parameter's data location to `calldata` to save gas.

APPENDIX | MANIFOLDXYZ

Finding Categories

Categories	Description
Gas Optimization	Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.
Coding Style	Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.
Inconsistency	Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER’S OR ANY OTHER PERSON’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

CertiK | Securing the Web3 World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.