Findings:

High:

1. ERC721A._burn(uint256,bool) contains an incorrect shift operation: _packedAddressData[from] += (1 << _BITPOS_NUMBER_BURNED) - 1

2. ERC721A._mint(address,uint256) contains an incorrect shift operation: _packedAddressData[to] += quantity * ((1 << _BITPOS_NUMBER_MINTED) | 1)

Medium:

1. ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes) ignores return value by lzEndpoint.estimateFees(_dstChainId,address(this),payload,_useZro,_adapterParams)
Recommendation: Ensure that all the return values of the function calls are used.

Low:

1. CyberSyndicate.purchaseTokens(uint256) uses timestamp for comparisons

- require(bool,string)(block.timestamp > publicmintActiveTime,The contract is paused)

Recommendation: Avoid relying on `block.timestamp`.

2. Reentrancy in ONFT721Core._send(address,uint16,bytes,uint256[],address,address,bytes)

- _lzSend(_dstChainId,payload,_refundAddress,_zroPaymentAddress,_adapterParams,msg.value)
- lzEndpoint.send{value: _nativeFee}(_dstChainId,trustedRemote,_payload,_refundAddress,_zroPaymentAddress,_adapterParams)
- SendToChain(_dstChainId,_from,_toAddress,_tokenIds)

Recommendation: Apply the [`check-effects-interactions` pattern](https://docs.soliditylang.org/en/latest/security-considerations.html#re-entrancy).

3. CyberSyndicate.baseExtension (Untitled-1.sol:3430) is never used in CyberSyndicate (Untitled-1.sol#3425-3564)

Recommendation: Remove unused state variables.

Informational:

1. Naming Conventions: there are some naming conversion errors in the source code. It may not cause in issue but it will be great if you choose some standard naming conventions. You can find solidity standard naming convensions on this link given below.
https://www.geeksforgeeks.org/solidity-style-guide/

Solidity Versions: Different versions of Solidity are used:

- **Version used:** ['>=0.5.0', '>=0.7.6', '>=0.8.0<0.9.0', '^0.8.0', '^0.8.13', '^0.8.17', '^0.8.4']

Recommendation: Use one Solidity version. Our Recommended version is 0.8.19. try not to use ^ symbol with solidity version.

Echidna Fuzz Testing

```
[2023-07-25 18:15:20.00] Compiling ./echidnaTest.sol... Done! (1.131590821s)
Analyzing contract: /home/shujagraphy/Desktop/Hardhat-boilerplate-main/Contracts/flaten/echidnaTest.sol:TestCyberSyndicate
[2023-07-25 18:15:21.27] Running slither on ./echidnaTest.sol... Done! (4.886881804s)
echidna_test_MintCost: passing
echidna_test_costPerNft: passing
echidna_test_totalMinted: passing
echidna_test_StartMintId: passing
echidna_test_OwnerMinted: passing


Unique instructions: 5596
Unique codehashes: 1
Corpus size: 1
Seed: 5626248097655294152
```

Slither Complete Report

```
'solc --version' running
'solc Untitled-1.sol --combined-json abi,ast,bin,bin-runtime,srcmap,srcmap-runtime,userdoc,devdoc,hashes --allow-paths
.,/home/shujagraphy/Desktop/Hardhat-boilerplate-main/Contracts/flaten' running
Compilation warnings/errors on Untitled-1.sol:
Warning: Contract code size is 27826 bytes and exceeds 24576 bytes (a limit introduced in Spurious Dragon). This contract may not be deployable on
Mainnet. Consider enabling the optimizer (with a low "runs" value!), turning off revert strings, or using libraries.
   --> Untitled-1.sol:3155:1:
    |
3155 | contract ONFT721A is ONFT721Core, ERC4907A, ERC721A__IERC721Receiver {
    | ^ (Relevant source part starts here and spans across multiple lines).

Warning: Contract code size is 34729 bytes and exceeds 24576 bytes (a limit introduced in Spurious Dragon). This contract may not be deployable on
Mainnet. Consider enabling the optimizer (with a low "runs" value!), turning off revert strings, or using libraries.
   --> Untitled-1.sol:3428:1:
    |
3428 | contract CyberSyndicate is Ownable, ERC2981, DefaultOperatorFilterer, ONFT721A {
    | ^ (Relevant source part starts here and spans across multiple lines).



INFO:Detectors:
ERC721A._mint(uint256,address) (Untitled-1.sol#1819-1877) contains an incorrect shift operation: _packedAddressData[to] += quantity * ((1 <<
_BITPOS_NUMBER_MINTED) | 1) (Untitled-1.sol#1834)
ERC721A._burn(bool,uint256) (Untitled-1.sol#1991-2058) contains an incorrect shift operation: _packedAddressData[from] += (1 <<
_BITPOS_NUMBER_BURNED) - 1 (Untitled-1.sol#2025)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-shift-in-assembly
INFO:Detectors:
BytesLib.concatStorage(bytes,bytes) (Untitled-1.sol#296-424) performs a multiplication on the result of a division:
        - sstore(uint256,uint256)(_preBytes,fslot_concatStorage_asm_0 + mload(uint256)(_postBytes + 0x20) / 0x100 ** 32 -
mlength_concatStorage_asm_0 * 0x100 ** 32 - newlength_concatStorage_asm_0 + mlength_concatStorage_asm_0 * 2) (Untitled-1.sol#320-345)
BytesLib.concatStorage(bytes,bytes) (Untitled-1.sol#296-424) performs a multiplication on the result of a division:
        - sstore(uint256,uint256)(sc_concatStorage_asm_0,mload(uint256)(mc_concatStorage_asm_0) / mask_concatStorage_asm_0 *
mask_concatStorage_asm_0) (Untitled-1.sol#389)
```

```
BytesLib.concatStorage(bytes,bytes) (Untitled-1.sol#296-424) performs a multiplication on the result of a division:
	- sstore(uint256,uint256)(sc_concatStorage_asm_0,mload(uint256)(mc_concatStorage_asm_0) / mask_concatStorage_asm_0 *
mask_concatStorage_asm_0) (Untitled-1.sol#421)
BytesLib.equalStorage(bytes,bytes) (Untitled-1.sol#626-689) performs a multiplication on the result of a division:
	- fslot_equalStorage_asm_0 = fslot_equalStorage_asm_0 / 0x100 * 0x100 (Untitled-1.sol#646)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes) (Untitled-1.sol#2966-2975) ignores return value by
lzEndpoint.estimateFees(_dstChainId,address(this),payload,_useZro,_adapterParams) (Untitled-1.sol#2974)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return
INFO:Detectors:
ONFT721A.constructor(string,string,uint256,address)._name (Untitled-1.sol#3156) shadows:
	- ERC721A._name (Untitled-1.sol#1211) (state variable)
ONFT721A.constructor(string,string,uint256,address)._symbol (Untitled-1.sol#3156) shadows:
	- ERC721A._symbol (Untitled-1.sol#1214) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
LzApp.setPrecrime(address)._precrime (Untitled-1.sol#2825) lacks a zero-check on :
		- precrime = _precrime (Untitled-1.sol#2826)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
ERC721A._checkContractOnERC721Received(address,address,uint256,bytes) (Untitled-1.sol#1786-1803) has external calls inside a loop: retval =
ERC721A__IERC721Receiver(to).onERC721Received(_msgSenderERC721A(),from,tokenId,_data) (Untitled-1.sol#1790-1802)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation/#calls-inside-a-loop
INFO:Detectors:
Reentrancy in ONFT721Core._send(address,uint16,bytes,uint256[],address,address,bytes) (Untitled-1.sol#3009-3036):
	External calls:
	- _lzSend(_dstChainId,payload,_refundAddress,_zroPaymentAddress,_adapterParams,msg.value) (Untitled-1.sol#3034)
		- lzEndpoint.send{value: _nativeFee}(_dstChainId,trustedRemote,_payload,_refundAddress,_zroPaymentAddress,_adapterParams)
(Untitled-1.sol#2745-2747)
	Event emitted after the call(s):
	- SendToChain(_dstChainId,_from,_toAddress,_tokenIds) (Untitled-1.sol#3035)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
```

```
CyberSyndicate.purchaseTokens(uint256) (Untitled-1.sol#3443-3450) uses timestamp for comparisons
	Dangerous comparisons:
	- require(bool,string)(block.timestamp > publicmintActiveTime,The contract is paused) (Untitled-1.sol#3444)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
ExcessivelySafeCall.excessivelySafeCall(address,uint256,uint16,bytes) (Untitled-1.sol#107-139) uses assembly
	- INLINE ASM (Untitled-1.sol#119-137)
ExcessivelySafeCall.excessivelySafeStaticCall(address,uint256,uint16,bytes) (Untitled-1.sol#156-188) uses assembly
	- INLINE ASM (Untitled-1.sol#169-186)
ExcessivelySafeCall.swapSelector(bytes4,bytes) (Untitled-1.sol#199-211) uses assembly
	- INLINE ASM (Untitled-1.sol#202-210)
BytesLib.concat(bytes,bytes) (Untitled-1.sol#226-294) uses assembly
	- INLINE ASM (Untitled-1.sol#229-291)
BytesLib.concatStorage(bytes,bytes) (Untitled-1.sol#296-424) uses assembly
	- INLINE ASM (Untitled-1.sol#297-423)
BytesLib.slice(bytes,uint256,uint256) (Untitled-1.sol#426-483) uses assembly
	- INLINE ASM (Untitled-1.sol#432-480)
BytesLib.toAddress(bytes,uint256) (Untitled-1.sol#485-494) uses assembly
	- INLINE ASM (Untitled-1.sol#489-491)
BytesLib.toUint8(bytes,uint256) (Untitled-1.sol#496-505) uses assembly
	- INLINE ASM (Untitled-1.sol#500-502)
BytesLib.toUint16(bytes,uint256) (Untitled-1.sol#507-516) uses assembly
	- INLINE ASM (Untitled-1.sol#511-513)
BytesLib.toUint32(bytes,uint256) (Untitled-1.sol#518-527) uses assembly
	- INLINE ASM (Untitled-1.sol#522-524)
BytesLib.toUint64(bytes,uint256) (Untitled-1.sol#529-538) uses assembly
	- INLINE ASM (Untitled-1.sol#533-535)
BytesLib.toUint96(bytes,uint256) (Untitled-1.sol#540-549) uses assembly
	- INLINE ASM (Untitled-1.sol#544-546)
BytesLib.toUint128(bytes,uint256) (Untitled-1.sol#551-560) uses assembly
	- INLINE ASM (Untitled-1.sol#555-557)
BytesLib.toUint256(bytes,uint256) (Untitled-1.sol#562-571) uses assembly
	- INLINE ASM (Untitled-1.sol#566-568)
BytesLib.toBytes32(bytes,uint256) (Untitled-1.sol#573-582) uses assembly
```

```
        - INLINE ASM (Untitled-1.sol#577-579)
BytesLib.equal(bytes,bytes) (Untitled-1.sol#584-624) uses assembly
        - INLINE ASM (Untitled-1.sol#587-621)
BytesLib.equalStorage(bytes,bytes) (Untitled-1.sol#626-689) uses assembly
        - INLINE ASM (Untitled-1.sol#629-686)
ERC721A._setAux(address,uint64) (Untitled-1.sol#1340-1349) uses assembly
        - INLINE ASM (Untitled-1.sol#1344-1346)
ERC721A._packOwnershipData(address,uint256) (Untitled-1.sol#1494-1501) uses assembly
        - INLINE ASM (Untitled-1.sol#1495-1500)
ERC721A._nextInitializedFlag(uint256) (Untitled-1.sol#1506-1512) uses assembly
        - INLINE ASM (Untitled-1.sol#1508-1511)
ERC721A._isSenderApprovedOrOwner(address,address,address) (Untitled-1.sol#1598-1611) uses assembly
        - INLINE ASM (Untitled-1.sol#1603-1610)
ERC721A._getApprovedSlotAndAddress(uint256) (Untitled-1.sol#1616-1627) uses assembly
        - INLINE ASM (Untitled-1.sol#1623-1626)
ERC721A.transferFrom(address,address,uint256) (Untitled-1.sol#1646-1702) uses assembly
        - INLINE ASM (Untitled-1.sol#1663-1668)
ERC721A._checkContractOnERC721Received(address,address,uint256,bytes) (Untitled-1.sol#1786-1803) uses assembly
        - INLINE ASM (Untitled-1.sol#1798-1800)
ERC721A._mint(uint256,address) (Untitled-1.sol#1819-1877) uses assembly
        - INLINE ASM (Untitled-1.sol#1851-1871)
ERC721A._burn(bool,uint256) (Untitled-1.sol#1991-2058) uses assembly
        - INLINE ASM (Untitled-1.sol#2008-2013)
ERC721A._setExtraDataAt(uint256,uint24) (Untitled-1.sol#2067-2077) uses assembly
        - INLINE ASM (Untitled-1.sol#2072-2074)
ERC721A._toString(uint256) (Untitled-1.sol#2120-2157) uses assembly
        - INLINE ASM (Untitled-1.sol#2121-2156)
ERC4907A.userOf(uint256) (Untitled-1.sol#2255-2269) uses assembly
        - INLINE ASM (Untitled-1.sol#2257-2267)
LzApp._getGasLimit(bytes) (Untitled-1.sol#2761-2766) uses assembly
        - INLINE ASM (Untitled-1.sol#2763-2765)
ONFT721Core._nonblockingLzReceive(uint16,bytes,uint64,bytes) (Untitled-1.sol#3038-3061) uses assembly
        - INLINE ASM (Untitled-1.sol#3048-3050)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Different versions of Solidity are used:
	- Version used: ['>=0.5.0', '>=0.7.6', '>=0.8.0<0.9.0', '^0.8.0', '^0.8.13', '^0.8.17', '^0.8.4']
	- >=0.5.0 (Untitled-1.sol#694)
	- >=0.5.0 (Untitled-1.sol#720)
	- >=0.5.0 (Untitled-1.sol#829)
	- >=0.5.0 (Untitled-1.sol#2324)
	- >=0.7.6 (Untitled-1.sol#87)
	- >=0.8.0<0.9.0 (Untitled-1.sol#223)
	- ^0.8.0 (Untitled-1.sol#10)
	- ^0.8.0 (Untitled-1.sol#2299)
	- ^0.8.0 (Untitled-1.sol#2417)
	- ^0.8.0 (Untitled-1.sol#2446)
	- ^0.8.0 (Untitled-1.sol#2471)
	- ^0.8.0 (Untitled-1.sol#2577)
	- ^0.8.0 (Untitled-1.sol#2603)
	- ^0.8.0 (Untitled-1.sol#2684)
	- ^0.8.0 (Untitled-1.sol#2850)
	- ^0.8.0 (Untitled-1.sol#2930)
	- ^0.8.13 (Untitled-1.sol#3180)
	- ^0.8.13 (Untitled-1.sol#3187)
	- ^0.8.13 (Untitled-1.sol#3328)
	- ^0.8.13 (Untitled-1.sol#3405)
	- ^0.8.17 (Untitled-1.sol#3422)
	- ^0.8.4 (Untitled-1.sol#846)
	- ^0.8.4 (Untitled-1.sol#1117)
	- ^0.8.4 (Untitled-1.sol#2165)
	- ^0.8.4 (Untitled-1.sol#2209)
	- ^0.8.4 (Untitled-1.sol#3144)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
INFO:Detectors:
ERC721A._mint(uint256,address) (Untitled-1.sol#1819-1877) has costly operations inside a loop:
	- _currentIndex = end (Untitled-1.sol#1874)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop
```

```
INFO:Detectors:
BytesLib.concat(bytes,bytes) (Untitled-1.sol#226-294) is never used and should be removed
BytesLib.concatStorage(bytes,bytes) (Untitled-1.sol#296-424) is never used and should be removed
BytesLib.equal(bytes,bytes) (Untitled-1.sol#584-624) is never used and should be removed
BytesLib.equalStorage(bytes,bytes) (Untitled-1.sol#626-689) is never used and should be removed
BytesLib.toAddress(bytes,uint256) (Untitled-1.sol#485-494) is never used and should be removed
BytesLib.toBytes32(bytes,uint256) (Untitled-1.sol#573-582) is never used and should be removed
BytesLib.toUint128(bytes,uint256) (Untitled-1.sol#551-560) is never used and should be removed
BytesLib.toUint16(bytes,uint256) (Untitled-1.sol#507-516) is never used and should be removed
BytesLib.toUint256(bytes,uint256) (Untitled-1.sol#562-571) is never used and should be removed
BytesLib.toUint32(bytes,uint256) (Untitled-1.sol#518-527) is never used and should be removed
BytesLib.toUint64(bytes,uint256) (Untitled-1.sol#529-538) is never used and should be removed
BytesLib.toUint8(bytes,uint256) (Untitled-1.sol#496-505) is never used and should be removed
BytesLib.toUint96(bytes,uint256) (Untitled-1.sol#540-549) is never used and should be removed
Context._msgData() (Untitled-1.sol#2594-2596) is never used and should be removed
ERC2981._deleteDefaultRoyalty() (Untitled-1.sol#2546-2548) is never used and should be removed
ERC2981._resetTokenRoyalty(uint256) (Untitled-1.sol#2568-2570) is never used and should be removed
ERC2981._setTokenRoyalty(uint256,address,uint96) (Untitled-1.sol#2558-2563) is never used and should be removed
ERC4907A._explicitUserOf(uint256) (Untitled-1.sol#2290-2292) is never used and should be removed
ERC721A._baseURI() (Untitled-1.sol#1406-1408) is never used and should be removed
ERC721A._burn(bool,uint256) (Untitled-1.sol#1991-2058) is never used and should be removed
ERC721A._burn(uint256) (Untitled-1.sol#1977-1979) is never used and should be removed
ERC721A._getAux(address) (Untitled-1.sol#1332-1334) is never used and should be removed
ERC721A._initializeOwnershipAt(uint256) (Untitled-1.sol#1443-1447) is never used and should be removed
ERC721A._mintERC2309(address,uint256) (Untitled-1.sol#1900-1930) is never used and should be removed
ERC721A._nextTokenId() (Untitled-1.sol#1268-1270) is never used and should be removed
ERC721A._numberBurned(address) (Untitled-1.sol#1325-1327) is never used and should be removed
ERC721A._numberMinted(address) (Untitled-1.sol#1318-1320) is never used and should be removed
ERC721A._ownershipAt(uint256) (Untitled-1.sol#1436-1438) is never used and should be removed
ERC721A._ownershipOf(uint256) (Untitled-1.sol#1429-1431) is never used and should be removed
ERC721A._setAux(address,uint64) (Untitled-1.sol#1340-1349) is never used and should be removed
ERC721A._setExtraDataAt(uint256,uint24) (Untitled-1.sol#2067-2077) is never used and should be removed
ERC721A._totalBurned() (Untitled-1.sol#1299-1301) is never used and should be removed
ERC721A._totalMinted() (Untitled-1.sol#1288-1294) is never used and should be removed
```

```
ERC721A._unpackedOwnership(uint256) (Untitled-1.sol#1484-1489) is never used and should be removed
ExcessivelySafeCall.excessivelySafeStaticCall(address,uint256,uint16,bytes) (Untitled-1.sol#156-188) is never used and should be removed
ExcessivelySafeCall.swapSelector(bytes4,bytes) (Untitled-1.sol#199-211) is never used and should be removed
ReentrancyGuard._reentrancyGuardEntered() (Untitled-1.sol#80-82) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.0 (Untitled-1.sol#10) allows old versions
Pragma version>=0.7.6 (Untitled-1.sol#87) allows old versions
Pragma version>=0.8.0<0.9.0 (Untitled-1.sol#223) is too complex
Pragma version>=0.5.0 (Untitled-1.sol#694) allows old versions
Pragma version>=0.5.0 (Untitled-1.sol#720) allows old versions
Pragma version>=0.5.0 (Untitled-1.sol#829) allows old versions
Pragma version^0.8.4 (Untitled-1.sol#846) allows old versions
Pragma version^0.8.4 (Untitled-1.sol#1117) allows old versions
Pragma version^0.8.4 (Untitled-1.sol#2165) allows old versions
Pragma version^0.8.4 (Untitled-1.sol#2209) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2299) allows old versions
Pragma version>=0.5.0 (Untitled-1.sol#2324) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2417) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2446) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2471) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2577) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2603) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2684) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2850) allows old versions
Pragma version^0.8.0 (Untitled-1.sol#2930) allows old versions
Pragma version^0.8.4 (Untitled-1.sol#3144) allows old versions
Pragma version^0.8.13 (Untitled-1.sol#3180) allows old versions
Pragma version^0.8.13 (Untitled-1.sol#3187) allows old versions
Pragma version^0.8.13 (Untitled-1.sol#3328) allows old versions
Pragma version^0.8.13 (Untitled-1.sol#3405) allows old versions
Pragma version^0.8.17 (Untitled-1.sol#3422) allows old versions
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

```
INFO:Detectors:
Low level call in CyberSyndicate.withdraw() (Untitled-1.sol#3490-3493):
	- (success) = address(msg.sender).call{value: address(this).balance}() (Untitled-1.sol#3491)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Parameter ExcessivelySafeCall.excessivelySafeCall(address,uint256,uint16,bytes)._target (Untitled-1.sol#107) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeCall(address,uint256,uint16,bytes)._gas (Untitled-1.sol#107) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeCall(address,uint256,uint16,bytes)._maxCopy (Untitled-1.sol#107) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeCall(address,uint256,uint16,bytes)._calldata (Untitled-1.sol#107) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeStaticCall(address,uint256,uint16,bytes)._target (Untitled-1.sol#156) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeStaticCall(address,uint256,uint16,bytes)._gas (Untitled-1.sol#156) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeStaticCall(address,uint256,uint16,bytes)._maxCopy (Untitled-1.sol#156) is not in mixedCase
Parameter ExcessivelySafeCall.excessivelySafeStaticCall(address,uint256,uint16,bytes)._calldata (Untitled-1.sol#156) is not in mixedCase
Parameter ExcessivelySafeCall.swapSelector(bytes4,bytes)._newSelector (Untitled-1.sol#199) is not in mixedCase
Parameter ExcessivelySafeCall.swapSelector(bytes4,bytes)._buf (Untitled-1.sol#199) is not in mixedCase
Parameter BytesLib.concat(bytes,bytes)._preBytes (Untitled-1.sol#226) is not in mixedCase
Parameter BytesLib.concat(bytes,bytes)._postBytes (Untitled-1.sol#226) is not in mixedCase
Parameter BytesLib.concatStorage(bytes,bytes)._preBytes (Untitled-1.sol#296) is not in mixedCase
Parameter BytesLib.concatStorage(bytes,bytes)._postBytes (Untitled-1.sol#296) is not in mixedCase
Parameter BytesLib.slice(bytes,uint256,uint256)._bytes (Untitled-1.sol#426) is not in mixedCase
Parameter BytesLib.slice(bytes,uint256,uint256)._start (Untitled-1.sol#426) is not in mixedCase
Parameter BytesLib.slice(bytes,uint256,uint256)._length (Untitled-1.sol#426) is not in mixedCase
Parameter BytesLib.toAddress(bytes,uint256)._bytes (Untitled-1.sol#485) is not in mixedCase
Parameter BytesLib.toAddress(bytes,uint256)._start (Untitled-1.sol#485) is not in mixedCase
Parameter BytesLib.toUint8(bytes,uint256)._bytes (Untitled-1.sol#496) is not in mixedCase
Parameter BytesLib.toUint8(bytes,uint256)._start (Untitled-1.sol#496) is not in mixedCase
Parameter BytesLib.toUint16(bytes,uint256)._bytes (Untitled-1.sol#507) is not in mixedCase
Parameter BytesLib.toUint16(bytes,uint256)._start (Untitled-1.sol#507) is not in mixedCase
Parameter BytesLib.toUint32(bytes,uint256)._bytes (Untitled-1.sol#518) is not in mixedCase
Parameter BytesLib.toUint32(bytes,uint256)._start (Untitled-1.sol#518) is not in mixedCase
Parameter BytesLib.toUint64(bytes,uint256)._bytes (Untitled-1.sol#529) is not in mixedCase
Parameter BytesLib.toUint64(bytes,uint256)._start (Untitled-1.sol#529) is not in mixedCase
Parameter BytesLib.toUint96(bytes,uint256)._bytes (Untitled-1.sol#540) is not in mixedCase
Parameter BytesLib.toUint96(bytes,uint256)._start (Untitled-1.sol#540) is not in mixedCase
Parameter BytesLib.toUint128(bytes,uint256)._bytes (Untitled-1.sol#551) is not in mixedCase
Parameter BytesLib.toUint128(bytes,uint256)._start (Untitled-1.sol#551) is not in mixedCase
Parameter BytesLib.toUint256(bytes,uint256)._bytes (Untitled-1.sol#562) is not in mixedCase
Parameter BytesLib.toUint256(bytes,uint256)._start (Untitled-1.sol#562) is not in mixedCase
Parameter BytesLib.toBytes32(bytes,uint256)._bytes (Untitled-1.sol#573) is not in mixedCase
Parameter BytesLib.toBytes32(bytes,uint256)._start (Untitled-1.sol#573) is not in mixedCase
Parameter BytesLib.equal(bytes,bytes)._preBytes (Untitled-1.sol#584) is not in mixedCase
Parameter BytesLib.equal(bytes,bytes)._postBytes (Untitled-1.sol#584) is not in mixedCase
Parameter BytesLib.equalStorage(bytes,bytes)._preBytes (Untitled-1.sol#626) is not in mixedCase
Parameter BytesLib.equalStorage(bytes,bytes)._postBytes (Untitled-1.sol#626) is not in mixedCase
Contract ERC721A__IERC721Receiver (Untitled-1.sol#1122-1126) is not in CapWords
Parameter ERC721A.safeTransferFrom(address,address,uint256,bytes)._data (Untitled-1.sol#1726) is not in mixedCase
Parameter LzApp.lzReceive(uint16,bytes,uint64,bytes)._srcChainId (Untitled-1.sol#2710) is not in mixedCase
Parameter LzApp.lzReceive(uint16,bytes,uint64,bytes)._srcAddress (Untitled-1.sol#2710) is not in mixedCase
Parameter LzApp.lzReceive(uint16,bytes,uint64,bytes)._nonce (Untitled-1.sol#2710) is not in mixedCase
Parameter LzApp.lzReceive(uint16,bytes,uint64,bytes)._payload (Untitled-1.sol#2710) is not in mixedCase
Parameter LzApp.getConfig(uint16,uint16,address,uint256)._version (Untitled-1.sol#2778) is not in mixedCase
Parameter LzApp.getConfig(uint16,uint16,address,uint256)._chainId (Untitled-1.sol#2778) is not in mixedCase
Parameter LzApp.getConfig(uint16,uint16,address,uint256)._configType (Untitled-1.sol#2778) is not in mixedCase
Parameter LzApp.setConfig(uint16,uint16,uint256,bytes)._version (Untitled-1.sol#2787) is not in mixedCase
Parameter LzApp.setConfig(uint16,uint16,uint256,bytes)._chainId (Untitled-1.sol#2787) is not in mixedCase
Parameter LzApp.setConfig(uint16,uint16,uint256,bytes)._configType (Untitled-1.sol#2787) is not in mixedCase
Parameter LzApp.setConfig(uint16,uint16,uint256,bytes)._config (Untitled-1.sol#2787) is not in mixedCase
Parameter LzApp.setSendVersion(uint16)._version (Untitled-1.sol#2795) is not in mixedCase
Parameter LzApp.setReceiveVersion(uint16)._version (Untitled-1.sol#2799) is not in mixedCase
Parameter LzApp.forceResumeReceive(uint16,bytes)._srcChainId (Untitled-1.sol#2803) is not in mixedCase
Parameter LzApp.forceResumeReceive(uint16,bytes)._srcAddress (Untitled-1.sol#2803) is not in mixedCase
Parameter LzApp.setTrustedRemote(uint16,bytes)._srcChainId (Untitled-1.sol#2809) is not in mixedCase
Parameter LzApp.setTrustedRemote(uint16,bytes)._path (Untitled-1.sol#2809) is not in mixedCase
Parameter LzApp.setTrustedRemoteAddress(uint16,bytes)._remoteChainId (Untitled-1.sol#2814) is not in mixedCase
Parameter LzApp.setTrustedRemoteAddress(uint16,bytes)._remoteAddress (Untitled-1.sol#2814) is not in mixedCase
Parameter LzApp.getTrustedRemoteAddress(uint16)._remoteChainId (Untitled-1.sol#2819) is not in mixedCase
Parameter LzApp.setPrecrime(address)._precrime (Untitled-1.sol#2825) is not in mixedCase
Parameter LzApp.setMinDstGas(uint16,uint16,uint256)._dstChainId (Untitled-1.sol#2830) is not in mixedCase
Parameter LzApp.setMinDstGas(uint16,uint16,uint256)._packetType (Untitled-1.sol#2830) is not in mixedCase
Parameter LzApp.setMinDstGas(uint16,uint16,uint256)._minGas (Untitled-1.sol#2830) is not in mixedCase
Parameter LzApp.setPayloadSizeLimit(uint16,uint256)._dstChainId (Untitled-1.sol#2837) is not in mixedCase
Parameter LzApp.setPayloadSizeLimit(uint16,uint256)._size (Untitled-1.sol#2837) is not in mixedCase
Parameter LzApp.isTrustedRemote(uint16,bytes)._srcChainId (Untitled-1.sol#2842) is not in mixedCase
Parameter LzApp.isTrustedRemote(uint16,bytes)._srcAddress (Untitled-1.sol#2842) is not in mixedCase
Parameter NonblockingLzApp.nonblockingLzReceive(uint16,bytes,uint64,bytes)._srcChainId (Untitled-1.sol#2896) is not in mixedCase
Parameter NonblockingLzApp.nonblockingLzReceive(uint16,bytes,uint64,bytes)._srcAddress (Untitled-1.sol#2897) is not in mixedCase
Parameter NonblockingLzApp.nonblockingLzReceive(uint16,bytes,uint64,bytes)._nonce (Untitled-1.sol#2898) is not in mixedCase
Parameter NonblockingLzApp.nonblockingLzReceive(uint16,bytes,uint64,bytes)._payload (Untitled-1.sol#2899) is not in mixedCase
Parameter NonblockingLzApp.retryMessage(uint16,bytes,uint64,bytes)._srcChainId (Untitled-1.sol#2911) is not in mixedCase
Parameter NonblockingLzApp.retryMessage(uint16,bytes,uint64,bytes)._srcAddress (Untitled-1.sol#2911) is not in mixedCase
Parameter NonblockingLzApp.retryMessage(uint16,bytes,uint64,bytes)._nonce (Untitled-1.sol#2911) is not in mixedCase
Parameter NonblockingLzApp.retryMessage(uint16,bytes,uint64,bytes)._payload (Untitled-1.sol#2911) is not in mixedCase
Parameter ONFT721Core.estimateSendFee(uint16,bytes,uint256,bool,bytes)._dstChainId (Untitled-1.sol#2957) is not in mixedCase
Parameter ONFT721Core.estimateSendFee(uint16,bytes,uint256,bool,bytes)._toAddress (Untitled-1.sol#2958) is not in mixedCase
Parameter ONFT721Core.estimateSendFee(uint16,bytes,uint256,bool,bytes)._tokenId (Untitled-1.sol#2959) is not in mixedCase
Parameter ONFT721Core.estimateSendFee(uint16,bytes,uint256,bool,bytes)._useZro (Untitled-1.sol#2960) is not in mixedCase
Parameter ONFT721Core.estimateSendFee(uint16,bytes,uint256,bool,bytes)._adapterParams (Untitled-1.sol#2961) is not in mixedCase
Parameter ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes)._dstChainId (Untitled-1.sol#2967) is not in mixedCase
Parameter ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes)._toAddress (Untitled-1.sol#2968) is not in mixedCase
Parameter ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes)._tokenIds (Untitled-1.sol#2969) is not in mixedCase
Parameter ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes)._useZro (Untitled-1.sol#2970) is not in mixedCase
Parameter ONFT721Core.estimateSendBatchFee(uint16,bytes,uint256[],bool,bytes)._adapterParams (Untitled-1.sol#2971) is not in mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._from (Untitled-1.sol#2978) is not in mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._dstChainId (Untitled-1.sol#2979) is not in mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._toAddress (Untitled-1.sol#2980) is not in mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._tokenId (Untitled-1.sol#2981) is not in mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._refundAddress (Untitled-1.sol#2982) is not in mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._zroPaymentAddress (Untitled-1.sol#2983) is not in
mixedCase
Parameter ONFT721Core.sendFrom(address,uint16,bytes,uint256,address,address,bytes)._adapterParams (Untitled-1.sol#2984) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._from (Untitled-1.sol#2998) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._dstChainId (Untitled-1.sol#2999) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._toAddress (Untitled-1.sol#3000) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._tokenIds (Untitled-1.sol#3001) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._refundAddress (Untitled-1.sol#3002) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._zroPaymentAddress (Untitled-1.sol#3003) is not in mixedCase
Parameter ONFT721Core.sendBatchFrom(address,uint16,bytes,uint256[],address,address,bytes)._adapterParams (Untitled-1.sol#3004) is not in mixedCase
Parameter ONFT721Core.clearCredits(bytes)._payload (Untitled-1.sol#3064) is not in mixedCase
Parameter ONFT721Core.setMinGasToTransferAndStore(uint256)._minGasToTransferAndStore (Untitled-1.sol#3110) is not in mixedCase
Parameter ONFT721Core.setDstChainIdToTransferGas(uint16,uint256)._dstChainId (Untitled-1.sol#3117) is not in mixedCase
Parameter ONFT721Core.setDstChainIdToTransferGas(uint16,uint256)._dstChainIdToTransferGas (Untitled-1.sol#3117) is not in mixedCase
Parameter ONFT721Core.setDstChainIdToBatchLimit(uint16,uint256)._dstChainId (Untitled-1.sol#3124) is not in mixedCase
Parameter ONFT721Core.setDstChainIdToBatchLimit(uint16,uint256)._dstChainIdToBatchLimit (Untitled-1.sol#3124) is not in mixedCase
Parameter CyberSyndicate.purchaseTokens(uint256)._mintAmount (Untitled-1.sol#3443) is not in mixedCase
Parameter CyberSyndicate.adminMint(address[],uint256)._sendNftsTo (Untitled-1.sol#3461) is not in mixedCase
Parameter CyberSyndicate.adminMint(address[],uint256)._howMany (Untitled-1.sol#3461) is not in mixedCase
Parameter CyberSyndicate.setnftsForOwner(uint256)._newnftsForOwner (Untitled-1.sol#3495) is not in mixedCase
Parameter CyberSyndicate.setDefaultRoyalty(address,uint96)._receiver (Untitled-1.sol#3499) is not in mixedCase
Parameter CyberSyndicate.setDefaultRoyalty(address,uint96)._feeNumerator (Untitled-1.sol#3499) is not in mixedCase
Parameter CyberSyndicate.setCostPerNft(uint256)._newCostPerNft (Untitled-1.sol#3503) is not in mixedCase
Parameter CyberSyndicate.setMetadataFolderIpfsLink(string)._newMetadataFolderIpfsLink (Untitled-1.sol#3507) is not in mixedCase
Parameter CyberSyndicate.setSaleActiveTime(uint256)._publicmintActiveTime (Untitled-1.sol#3511) is not in mixedCase
Constant CyberSyndicate.baseExtension (Untitled-1.sol#3433) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
ExcessivelySafeCall.slitherConstructorConstantVariables() (Untitled-1.sol#89-212) uses literals with too many digits:
	- LOW_28_MASK = 0x00000000ffffffffffffffffffffffffffffffffffffffffffffffffffffffff (Untitled-1.sol#90)
BytesLib.toAddress(bytes,uint256) (Untitled-1.sol#485-494) uses literals with too many digits:
	- tempAddress = mload(uint256)(_bytes + 0x20 + _start) / 0x1000000000000000000000000 (Untitled-1.sol#490)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
```

```
CyberSyndicate.baseExtension (Untitled-1.sol#3433) is never used in CyberSyndicate (Untitled-1.sol#3428-3567)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable
INFO:Detectors:
CyberSyndicate.maxSupply (Untitled-1.sol#3429) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Slither:Untitled-1.sol analyzed (27 contracts with 88 detectors), 232 result(s) found
```

Note: we analyze this report after flatten the main contract.