

Smart contract vulnerabilities assessment report



Date: 12 December 2024

Project: Open source dynamic assets (Token/ NFT) generator (CIP68)

Version: 1.0

Created by: Tien Nguyen Anh

Disclosure

This document contains proprietary information belonging to cardano2vn.io. Duplication, redistribution, or use, in whole or in part, in any form, requires explicit consent from Ancardano2vn.io.

Nonetheless, both the customer cardano2vn and our partners are authorized to share this document with the public to demonstrate security compliance and transparency regarding the outcomes of the Protocol.

Disclaimer and Scope

Our code review represents a snapshot in time, and the findings and recommendations presented in this report reflect the information gathered during the assessment period. It is important to note that any modifications made outside of this timeframe will not be captured in this report.

While diligent efforts have been made to uncover potential vulnerabilities, it is essential to recognize that this assessment may not uncover all potential security issues in the protocol.

It is imperative to understand that the findings and recommendations provided in this audit report should not be construed as investment advice.

Furthermore, it is strongly recommended that projects consider undergoing multiple independent audits and/or participating in bug bounty programs to increase their protocol security.

Please be aware that the scope of this security audit does not extend to the compiler layer, such as the UPLC code generated by the compiler or any areas beyond the audited code.

The scope of the assessment did not include additional creation of unit testing or property-based testing of the contracts.

Version control

Version	Date	Author	Update note
1.0	12 Dec 2024	Tien Nguyen Anh	First draft
1.1	14 Dec 2024	Tien Nguyen Anh	Second update (update and burnt test)

Assessment overview

This review is intended to confirm that the smart contract features work well and avoid basic bugs before being released to the public for bug hunting.

The review is conducted from December 12, 2024 to December 16, 2024

Assessment components

The assessments are performed only with 02 validators, mint and store, and do not include other related components.

Code base

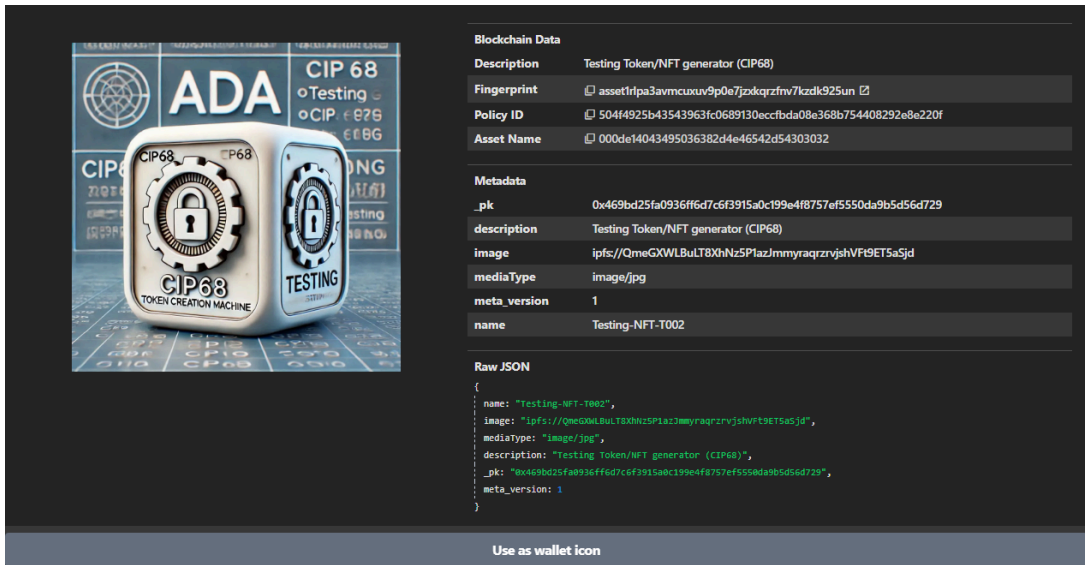
FUNCTION	MINTING
repository	https://github.com/cardano2vn/cip68generator
commit	09ca522ff1a2778e4fce5ee1e44553f920db19c0
File audit	https://github.com/cardano2vn/cip68generator/blob/main/contract/validators/mint.ak

FUNCTION	UPDATE AND BURNT
repository	https://github.com/cardano2vn/cip68generator
commit	4af7ec9e7e0bf46c2c4bb606c2039b749caf2796
File audit	https://github.com/cardano2vn/cip68generator/blob/main/contract/validators/store.ak

Severity Classification

- **Critical:** This vulnerability has the potential to result in significant financial losses. They often enable attackers to directly steal assets from contracts or users, or permanently lock funds within the contract.
- **Major:** Can lead to damage to the user or platform although the impact may be restricted to specific functionalities or temporal control. Attackers exploiting major vulnerabilities may cause harm or disrupt certain aspects of the platform.
- **Medium:** May not directly result in financial losses, but they can temporarily impair the platform's functionality. Examples include susceptibility to front-running attacks, which can undermine the integrity of transactions.
- **Minor:** Minor vulnerabilities do not typically result in financial losses or significant harm to users or the platform. The attack vector may be inconsequential or the attacker's incentive to exploit it may be minimal.
- **Informational:** These findings do not pose immediate financial risks. These may include platform optimizations, code style recommendations, alignment with naming conventions, overall contract design suggestions, and documentation discrepancies between the code

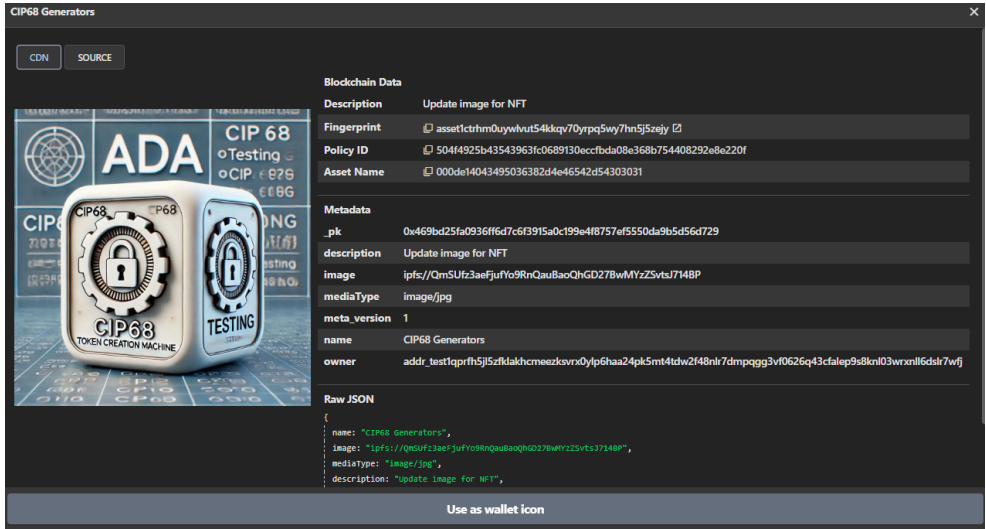
Test case and findings:

Testcase_ID	ID_mint_001	Function	Mint
Severity	Informational	Status	Resolve
Description	Provide enough information to test mint function operation in mint validator		
Purpose	Test mint function performance under normal conditions		
Evidence	<p>https://preview.cexplorer.io/tx/8d5b41276abf701d1a0a27fd9a6fc37a7dc75a0174181d6cf66bff0d5410a7a5</p> <p>Image which is taken from Eternl wallet</p> 		
Findings:	transaction executes fine and returns tx_hash as expected		

Testcase_ID	ID_mint_002	Function	Mint
Severity	Informational	Status	Resolve
Description	Provide the same token name and description as the token just created		
Purpose	To check if the validator recognizes the created token		

Evidence	<p style="text-align: center;">^</p> <p>error: Tx evaluation failed:</p> <pre>{ "type": "jsonwsp/response", "version": "1.0", "servicename": "ogmios", "method name": "EvaluateTx", "result": { "EvaluationFailure": { "ScriptFailures": { "spend:1": { "missingRequiredScripts": { "missing": ["spend:1"] } } } }, "reflection": { "id": "2953c2b3-b343-4333-a5d9-1be2ee3be9b3" } } }</pre> <p>For txHex:</p> <pre>84a800d9010282825820430a5d9c37c8c947c6aa333e6895fcb6922bdb488c26e03b07ed 9aab5b17ddea018258208d5b41276abf701d1a0a27fd9a6fc37a7dc75a0174181d6cf66bf f0d5410a7a5010184a300581d70d8732d3c7113002857e0cf983faea841ae0bd1e6cfdad1 fe6cb4eb0301821a001f5ebea1581c504f4925b43543963fc0689130eccfbda08e368b7544 08292e8e220fa152000643b043495036382d4e46542d5430303101028201d81858bed879 9fa5446e616d654e43495036382d4e46542d5430303145696d6167655835697066733a2f 2f516d654758574c42754c543858684e7a355031617a4a6d6d79726171727a72766a7368 5646743945543561536a64496d656469615479706549696d6167652f6a70674b64657363 72697074696f6e582354657374696e6720546f6b656e2f4e46542067656e657261746f722 028434950363829435f706b581c469bd25fa0936ff6d7c6f3915a0c199e4f8757ef5550da9 b5d56d72901ff82583900469bd25fa0936ff6d7c6f3915a0c199e4f8757ef5550da9b5d56d 729353cfe3f376102111625fa568158e13dfe42581ed3fbe2e19a7ffe9b821a00124864a15 81c504f4925b43543963fc0689130eccfbda08e368b754408292e8e220fa152000de140434 95036382d4e46542d543030310182583900a421f93124a36acac4f4317c5280963fd76937 c444998fa3df4bf8d3c5bbb83198aef72e22944dc453bd89d9feafdc55f51108e97e92bcff1 a000f424082583900469bd25fa0936ff6d7c6f3915a0c199e4f8757ef5550da9b5d56d7293 53cfe3f376102111625fa568158e13dfe42581ed3fbe2e19a7ffe9b1a00b4dfe3021a0016b a2b09a1581c504f4925b43543963fc0689130eccfbda08e368b754408292e8e220fa15200 0de14043495036382d4e46542d54303031010b5820419cf0bd66b478f1491b8ce4c00064 cdf47657915e6c9320a964c89ed66658380dd9010281825820c1f8bd2f7ab0f98889947c7 a4b1015d293c6df4e8f16784fbc268b02ef3832dd000ed9010281581c469bd25fa0936ff6d 7c6f3915a0c199e4f8757ef5550da9b5d56d72912d90102818258204e25c9426adf5f0eaa9 1d34e2fbb414101d580cc42a682a1698cfda78f48fdd800a105a282000182d87980821a00 6acfc01ab2d05e0082010082d87980821a006acfc01ab2d05e00f5f6</pre> <p>at</p> <p>/home/cardano/aikenlabs/cip68generator/node_modules/@meshsdk/transaction/dist/index.js:1666:15</p> <p>✗ Mint, Burn, Update, Remove Assets (NFT/TOKEN) CIP68 > Mint [1152.45ms]</p> <p>0 pass</p>
----------	--

	1 fail Ran 1 tests across 1 files. [3.76s]
Findings	Smart contract refuses to create existing token, transaction error

Testcase_ID	ID_mint_003	Function	Update
Severity	Informational	Status	Resolve
Description	provide the transaction with the name of the token and the metadata to be changed		
Purpose	Test smart contract's ability to update token metadata		
Evidence	<p>https://preview.cexplorer.io/tx/a5c3f917759afeb3495c03faba693154443b18dc4e1937ebc97a033a59a34e6a</p> <p>The image which is captured from Eternl wallet</p> 		
Findings	The transaction executed successfully and returned tx_hash, metadata was update as expected.		

Testcase_ID	ID_mint_004	Function	Update
-------------	-------------	----------	--------

Severity	Informational	Status	Resolve
Description	Update token Metadata content with another wallet, not the wallet that minted token		
Purpose	To check whether the Smart Contract condition confirms the token owner or not		
Evidence	<pre> 1661 this.meshTxBuilderBody, 1662 this._protocolParams 1663); 1664 if (this.evaluator) { 1665 const txEvaluation = await this.evaluator.evaluateTx(txHex).catch((error) => { 1666 throw Error(`Tx evaluation failed: \${error} ^ error: Tx evaluation failed: {"type":"jsonwsp/response","version":"1.0","servicename":"ogmios","methodname":"EvaluateTx","result":{"EvaluationFailure":{"ScriptFailures":{}}},"reflection":{"id":"295c0423-369c-4170-99db-53a79bb74974"}} For txHex: 84a700d9010282825820385b7bb98561977177324ca340f013b09f5f1ca34ea094e10555a 3e6936bb57703825820a5c3f917759afeb3495c03faba693154443b18dc4e1937ebc97a03 3a59a34e6a000183a300581d70d8732d3c7113002857e0cf983faea841ae0bd1e6cfdad1fe 6cb4eb0301821a0027eb6aa1581c504f4925b43543963fc0689130eccfbda08e368b754408 292e8e220fa152000643b043495036382d4e46542d5430303101028201d81859013fd8799 fa6446e616d655043495036382047656e657261746f727345696d6167655835697066733a 2f2f516d5355667a336165466a7566596f39526e51617542616f51684744323742774d597a 5a537674734a3731344250496d656469615479706549696d6167652f6a70674b646573637 2697074696f6e582a55706461746520696d61676520666f72204e4654206279207573696e 67206f746865722077616c6c6574456f776e65725f5840616464725f746573743171716577 366a617a36337533383967776e7038773932716e7465747a7873366a39323232706e34636 e656a36373276617a7337613677582c6e7273657167676a34643475723433797139653233 723471306d3837397437656679687a6a71386d767a7561ff435f706b581c32ed4ba2d4791 3950e984ee2a8135e562343522a94a0ceb89e65af2901ff82583900a421f93124a36acac4f4 317c5280963fd76937c444998fa3df4bf8d3c5bbb83198aef72e22944dc453bd89d9feafdc 55f51108e97e92bcff1a000f42408258390032ed4ba2d47913950e984ee2a8135e56234352 2a94a0ceb89e65af299d143ddd3a638640844aadaf07589005caa23a81fb3f8abf6524b8a4 1a10c80774021a000ccfd80b5820e5a9393365e82f189cc71b0446e9da64951f537a5ed762 </pre>		

	a685a5403c2e4c30690dd9010281825820dc451e481a3ed20be5a509693ca92b85eed468 b0fbad3271e84bd6be09a14868020ed9010281581c32ed4ba2d47913950e984ee2a8135e 562343522a94a0ceb89e65af2912d901028182582059143e9cc9ed0139283559fe253b894 0937dc49a45bb972da27e9cd764113b0200a105a182000182d87980821a006acfc01ab2d 05e00f5f6 at /home/cardano/aikenlabs/cip68generator/node_modules/@meshsdk/transaction/dist/i ndex.js:1666:15 ✗ Mint, Burn, Update, Remove Assets (NFT/TOKEN) CIP68 > Update [1538.41ms] 0 pass 1 fail Ran 1 tests across 1 files. [3.54s]
Findings	The tx could not be authenticated and failed as expected.

Testcase_ID	ID_mint_005	Function	Burnt
Severity	Informational	Status	Resolve
Description	perform token burning with a wallet other than the owner's wallet		
Purpose	perform token burning with a wallet other than the owner's wallet		
Evidence	cardano@did-client:~/aikenlabs/cip68generator\$ bun test bun test v1.1.38 (bf2f153f) 276 module.exports.js_serialize_tx_body = function(tx_builder_body_json, params_json) { 277 const ptr0 = passStringToWasm0(tx_builder_body_json, wasm.__wbindgen_malloc, wasm.__wbindgen_realloc); 278 const len0 = WASM_VECTOR_LEN; 279 const ptr1 = passStringToWasm0(params_json, wasm.__wbindgen_malloc, wasm.__wbindgen_realloc);		

	<pre> 280 const len1 = WASM_VECTOR_LEN; 281 const ret = wasm.js_serialize_tx_body(ptr0, len0, ptr1, len1); ^ RuntimeError: Unreachable code should not be executed (evaluating 'wasm.js_serialize_tx_body(ptr0, len0, ptr1, len1)') at <?>.wasm-function[3555] at <?>.wasm-function[5004] at <?>.wasm-function[4575] at <?>.wasm-function[627] at <?>.wasm-function[4018] at /home/cardano/aikenlabs/cip68generator/node_modules/@sidan-lab/sidan-csl-rs-node js/sidan_csl_rs.js:281:22 at serializeTxBody (/home/cardano/aikenlabs/cip68generator/node_modules/@meshsdk/core-csl/dist/ind ex.js:1178:31) at /home/cardano/aikenlabs/cip68generator/node_modules/@meshsdk/transaction/dist/i ndex.js:1660:33 ✗ Mint, Burn, Update, Remove Assets (NFT/TOKEN) CIP68 > Burn [1201.40ms] 1 fail Ran 2 tests across 1 files. [3.31s] cardano@did-client:~/aikenlabs/cip68generator\$ </pre>
Findings	Transaction returned error

Testcase_ID	ID_mint_005	Function	Burnt
Severity	Informational	Status	Resolve
Description	To evaluate the possibility of burning tokens and SC checks the terms of the token owners who are burned		



Purpose	To evaluate whether the Smart Contract's binding conditions check the token owner's conditions or not
Evidence	<pre>cardano@did-client:~/aikenlabs/cip68generator\$ bun test bun test v1.1.38 (bf2f153f)</pre> <p>contract/tests/cip68.test.ts:</p> <ul style="list-style-type: none">✓ Mint, Burn, Update, Remove Assets (NFT/TOKEN) CIP68 > Update [0.25ms] <p>https://preview.cexplorer.io/tx/2353476cf78cb3ad2ef8e1601ab7c64db54c8a1f32c8781240285e4be6c72203</p> <ul style="list-style-type: none">✓ Mint, Burn, Update, Remove Assets (NFT/TOKEN) CIP68 > Burn [1623.45ms] <p>2 pass 0 fail 1 expect() calls Ran 2 tests across 1 files. [4.87s]</p>
Findings	The transaction executed successfully and returned tx_hash