Cyberscope

Audit Report

Empowa

May 2025

Network	Cardano
Fingerprint	asset1u898rd424aqyuc4g6vdkhxh5hu86zcv2jc60ju
Policy	6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81
Audited by	© cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Token Explorer	https://cardanoscan.io/token/6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81456d706f7761
Policy Explorer	https://cardanoscan.io/tokenPolicy/6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81
Fingerprint	asset1u898rd424aqyuc4g6vdkhxh5hu86zcv2jc60ju
Policy Id	6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81
Network	Cardano
Name (Hex)	Empowa (456d706f7761)
Ticker	EMP
Decimals	6
Total Supply	200,000,000

Audit Updates

Initial Audit	28 May 2025

Overview

Empowa (EMP) is a fungible native token on the Cardano blockchain. As this asset is a native token, the ledger itself handles the token's logic such as transferring and managing and monitoring balances. Empowa is set under the rules of its minting policy, with id `6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81` , which was created at the same time the token was minted for the first time. The creation slot was `55779258` in epoch `326` .


```
{
  all: [
    {
      invalidAfter: 56764800

    },
    {
      pubKeyHash:
"ce97829133eee82cf84d9b4e05cd3d873787d1ee8777086619f8de0e"

    }
  ]
}
```


The policy script enables a set of rules for any native token that is associated with it. Specifically, this policy script enables a time-locked mint/burn policy. This means that the `pubKeyHash` `ce97829133eee82cf84d9b4e05cd3d873787d1ee8777086619f8de0e` is able to mint or burn tokens as long as the current slot is less than the `invalidAfter` property which is equal to `56764800` (approximately 11 days after its creation). It is worth noting that no other entity is able to mint and burn tokens under this policy.

The token has been minted twice with the first occurrence at creation, slot `55779258`, where a total of `200` EMP tokens were minted. The transaction associated with the token's creation can be found here.

The second instance occurred at slot `55835723` where `199_999_800` EMP tokens were minted making the total amount of EMP tokens equal to `200_000_000` . The hash for this transaction can be found here.

Since the current slot is greater than `invalidAfter` property established at the policy, the token can never be minted again, permanently locking it to the total supply of `200_000_000` EMP tokens.

Metadata

The metadata for the Empowa token on the Cardano blockchain provides essential details about this digital asset, facilitating its integration and operation within the ecosystem. The metadata includes crucial information that defines the token's characteristics and ensures its seamless functionality across the network.

On-Chain Metadata

The on-chain metadata were initially created when the token was first minted and were not changed thereafter.


```
{
  "6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81":{
    "456d706f7761":{
      "ref":"https://token.empowa.io/emp"
    }
  }
}
```


The metadata signify that the token `456d706f7761` (which is the hex representation of its name, `Empowa`) of the policy with id `6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81` is linked with the following ref: https://token.empowa.io/emp. Further investigating this link reveals the off-chain metadata of the token.

```
{
  "20":{
    "6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81":{
      "456d706f7761":{
        "ticker":"EMP",
        "url":"https://empowa.io",
        "desc":"Empowa is the first RealFi property platform on Cardano
that combines emerging technology, sustainable building and decentralised
financial inclusion. The Empowa utility token (EMP) allows different
parties to participate in the Empowa ecosystem using a common unit of
value.",
        "icon":"https://token.empowa.io/emp/icon.png",
        "decimals":"6"
      }
    }
  }
}
```


At the time of conducting this audit, the off-chain metadata includes some of the token's key features such as its `ticker` , `EMP` , the `url` associated with the protocol as well as the protocol's description. Additionally, the metadata also reveals the icon which is the visual representation of the token. Lastly, the token has `6` decimal points, as signified by the metadata, a very useful information for external applications that interact with the token.

Token Registry Metadata

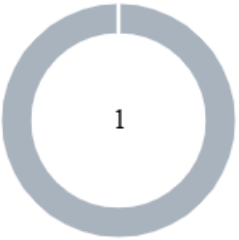
The token has additionally registered metadata to the Cardano Foundation's Token Registry and can be found under the commit `dfd4ea11ce814e244fc6d9198e0ba0fd01027cc4` of the repository provided in this link. This makes the token easily identified, tracked, and verified within the Cardano ecosystem.

```
{
    "subject":
"6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81456d706f7761",
    "url": {
        "sequenceNumber": 0,
        "value": "https://empowa.io",
        "signatures": [
            {
                "signature": "81823549a7edd8…dbd81f200",
                "publicKey":
"b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b"
            }
        ]
    },
    "name": {
        "sequenceNumber": 0,
        "value": "Empowa",
        "signatures": [
            {
                "signature": "911ec6b6ea4c4…610f67731eaa904",
                "publicKey":
"b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b"
            }
        ]
    },
    "ticker": {
        "sequenceNumber": 0,
        "value": "EMP",
        "signatures": [
            {
                "signature": "56f8be84a633dc9…6f732241d3000",
                "publicKey":
"b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b"
            }
        ]
    },
    "decimals": {
        "sequenceNumber": 0,
        "value": 6,
        "signatures": [
            {
                "signature": "040a8440960a6…065735f50a",
                "publicKey":
"b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b"
            }
        ]
    },
    "policy":
"820182018282051a036229808200581cce97829133eee82cf84d9b4e05cd3d873787d1ee
8777086619f8de0e",
```

```
    "logo": {
        "sequenceNumber": 0,
        "value": "iVBORw0KGgoAAAANSUhEUgAAAgEAAAIBCAYA...",
        "signatures": [
            {
                "signature": "ae39996036f356…4735e0d5eaed104",
                "publicKey":
"b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b"
            }
        ]
    },
    "description": {
        "sequenceNumber": 1,
        "value": "Empowa is the first RealFi property platform on Cardano
that combines emerging technology, sustainable building and decentralised
financial inclusion. The Empowa utility token (EMP) allows different
parties to participate in the Empowa ecosystem using a common unit of
value.",
        "signatures": [
            {
                "signature": "ca7d22fbd…043dedc538f74acd604a9202",
                "publicKey":
"b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b"
            }
        ]
    }
}
```


The registry metadata reveals similar information as the metadata associated with on-chain stored link. Additional information include the name of the token that can also be found on-chain but not on the metadata as well as the logo which is the base 64 representation of the token's icon. All the information stored in the token registry are also signed by the same `publicKey` : `b63a5ba819d57b259ef23edd22e76f038a4fa57c26d17b23f553e64da10f4a2b` .

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	1	0	0	0

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	UA	Update Authority	Unresolved

MA - Mint Authority

Criticality	Passed
Status	Resolved

Description

The entity associated with the `pubKeyHash` mentioned in the policy script has the authority to mint tokens at their discretion, allowing them to create new tokens until the `56764800` slot has passed. This centralizes control over the token supply, as they can increase the total supply at will. Such a design underscores the importance of trust in that entity's actions and transparency in their decision-making, as these actions can directly influence the token's scarcity, value, and overall ecosystem. Slot `56764800` has been reached and as a result, the entity no longer has the authority to mint tokens. Consequently, the total supply is permanently locked at a total of `200,000,000` tokens.

```
{
   all: [
      {
         invalidAfter: 56764800
      },
      {
         pubKeyHash:
"ce97829133eee82cf84d9b4e05cd3d873787d1ee8777086619f8de0e"
      }
   ]
}
```

UA - Update Authority

Criticality	Minor / Informative
Status	Unresolved

Description

The token's metadata points to an external link which in turn points to a centralized server. This means that the token's metadata can be changed from the owner of the server. This provides centralized control over token properties. Additionally, the token's metadata stored in the registry can also be altered. This feature introduces the risk of misuse, which could lead to changes that undermine trust in the token's integrity or utility.

```
{
    "6c8642400e8437f737eb86df0fc8a8437c760f48592b1ba8f5767e81":{
        "456d706f7761":{
            "ref":"https://token.empowa.io/emp"
        }
    }
}
```

Recommendation

It is recommended that the metadata are stored on-chain or in decentralized storages. This will enhance the trust of its holders and will incentivise more users to interact with the protocol.

Summary

The Empowa token, built on the Cardano network, leverages a solid architecture. This audit rigorously evaluates its performance, security, and compliance with best practices. The investigation aims to identify and address any operational vulnerabilities, performance bottlenecks, and areas for optimization, ensuring the token's robustness and reliability in the Cardano ecosystem.

The token can no longer be minted due to the time locked limitation in its policy that renders the policy locked after the `slot 56764800`. As of the time of this audit the current slot is `156959441`.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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 Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope'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 Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

cyberscope.io