

The logo for DeHacker, featuring the word "DeHacker" in a bold, sans-serif font. The "De" is in a light blue color, and "Hacker" is in a darker blue. The background of the slide is black with a series of concentric circles in a light blue color, creating a ripple effect. There are also some blurred light blue spots in the corners.

DeHacker

Code Security Assessment

Iskra - ItemNFTSnapshot

Sep 6th, 2023



Contents

CONTENTS	1
SUMMARY	2
ISSUE CATEGORIES	3
OVERVIEW	4
PROJECT SUMMARY	4
VULNERABILITY SUMMARY	4
AUDIT SCOPE	5
FINDINGS	6
MAJOR.....	7
INF-01 CENTRALIZATION RISKS IN ITEMNFTSNAPSHOT.SOL	7
DESCRIPTION	7
RECOMMENDATION	8
INFORMATIONAL.....	9
INF-04 MISSING EMIT EVENTS	9
DESCRIPTION	9
RECOMMENDATION	9
INFORMATIONAL.....	10
INF-06 BATCHMINTING DOES NOT PREVENT OVERFLOW	10
DESCRIPTION	10
RECOMMENDATION	10
DISCLAIMER.....	11
APPENDIX.....	12
ABOUT.....	13



Summary

DeHacker's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow/underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service/logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting



Issue Categories

Every issue in this report was assigned a severity level from the following:

Critical severity issues

A vulnerability that can disrupt the contract functioning in a number of scenarios or creates a risk that the contract may be broken.

Major severity issues

A vulnerability that affects the desired outcome when using a contract or provides the opportunity to use a contract in an unintended way.

Medium severity issues

A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.

Minor severity issues

A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.

Informational

A vulnerability that has informational character but is not affecting any of the code.



Overview

Project Summary

Project Name	Iskra - ItemNFTSnapshot
Platform	Ethereum
Website	https://iskra.world/
Type	NFT
Language	Solidity

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	1	0	0	1	0	0
Medium	0	0	0	0	0	0
Minor	0	0	0	0	0	0
Informational	2	0	0	1	0	1
Discussion	0	0	0	0	0	0



Audit scope

ID	File	SHA256 Checksum
INF	contracts/token/ERC721/ ItemNFTSnapshot.sol	4889f01714a244b6a25b7492c5bfd6c5 a1842a9d187f5d4e1bb44799567f1cee
ERC	contracts/token/ERC721/ extensions/ ERC721Snapshot.sol	20e0c51159a5ec97a11888a20a82337a 7a08457e1714f6b37bb2d9ec0876a902



Findings

ID	Category	Severity	Status
INF-01	Centralization	Major	Acknowledged
INF-04	Coding Style	Informational	Resolved
INF-06	Volatile Code	Informational	Acknowledged



MAJOR

INF-01|CENTRALIZATION RISKS IN ITEMNFTSNAPSHOT.SOL

Category	Severity	Location	Status
Centralization	Major	contracts/token/ ERC721/ ItemNFTSnapshot. sol : 113, 122, 127, 147	Acknowledged

Description

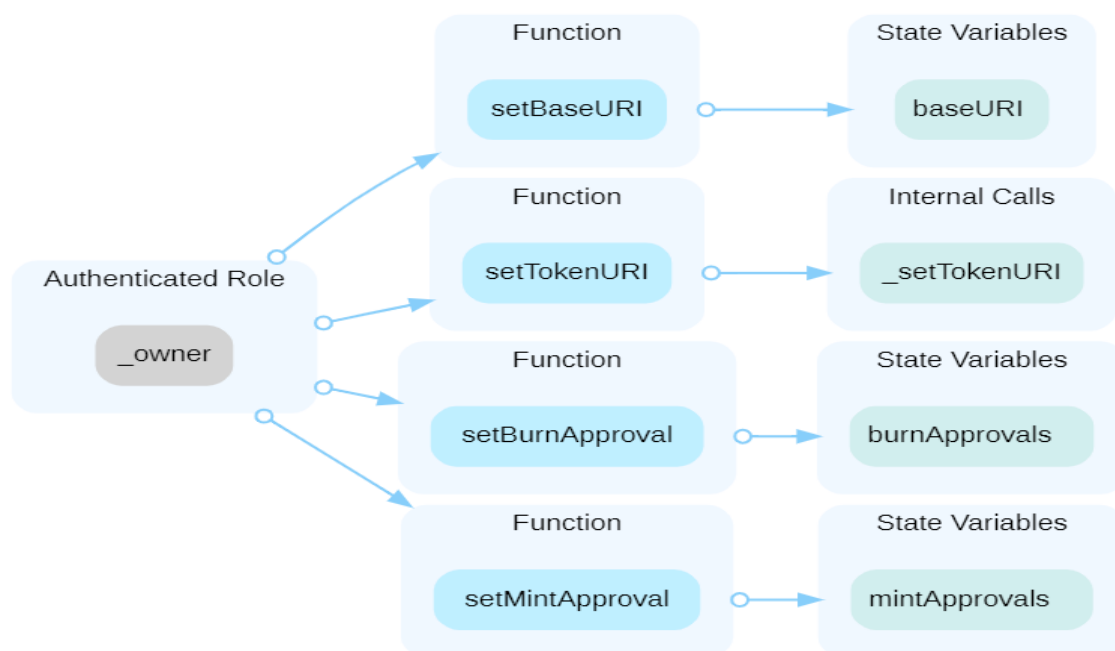
In the contract ItemNFTSnapshot the role `_owner` has authority over the functions shown in the diagram below.

Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and :

grant or revoke the capacity to mint tokens to any address;

grant or revoke the capacity to burn tokens to any address (if the contract has been deployed as burnable);

change the URI;





Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (,) combination mitigate by delaying the sensitive operation and avoiding a single point of key management failure.

Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;

AND

Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;

AND

A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, mitigate by applying decentralization and transparency.

Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;

AND

Introduction of a DAO/governance/voting module to increase transparency and user involvement.

AND

A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered fully resolved.

Renounce the ownership and never claim back the privileged roles.

OR

Remove the risky functionality.



INFORMATIONAL

INF-04 | MISSING EMIT EVENTS

Category	Severity	Location	Status
Coding Style	Informational	contracts/token/ERC721/ItemNFTSnapshot.sol (6c975f1183c2609b395e0ac94b8163b6dce23604): 147	Resolved

Description

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.



INFORMATIONAL

INF-06|BATCHMINTING DOES NOT PREVENT OVERFLOW

Category	Severity	Location	Status
Volatile Code	Informational	contracts/token/ERC721/ItemNFTSnapshot.sol (6c975f1183c2609b395e0ac94b8163b6dce23604): 88~89	Acknowledged

Description

The function ERC721._mint() updates the receiver balance as follows:

```
unchecked {  
    // Will not overflow unless all 2**256 token ids are minted to the same  
owner.  
    // Given that tokens are minted one by one, it is impossible in practice  
that  
    // this ever happens. Might change if we allow batch minting.  
    // The ERC fails to describe this case.  
    _balances[to] += 1;  
}
```

In theory, the function safeMintBatch() could cause an overflow.

Recommendation

We recommend adding checks to prevent balance overflow.



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. Blockchain 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.



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Coding Style

Coding Style findings usually do not affect the generated bytecode but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

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.



About

DeHacker is a team of auditors and white hat hackers who perform security audits and assessments. With decades of experience in security and distributed systems, our experts focus on the ins and outs of system security. Our services follow clear and prudent industry standards. Whether it's reviewing the smallest modifications or a new platform, we'll provide an in-depth security survey at every stage of your company's project. We provide comprehensive vulnerability reports and identify structural inefficiencies in smart contract code, combining high-end security research with a real-world attacker mindset to reduce risk and harden code.

BLOCKCHAINS



Ethereum



Cosmos



Eos



Substrate

TECH STACK



Python



Rust



Solidity



C++

CONTACTS

<https://dehacker.io><https://twitter.com/dehackerio>https://github.com/dehacker/audits_public<https://t.me/dehackerio><https://blog.dehacker.io/>



DeHacker

Sep 2023