macro

Cannon A-1

Security Audit

June 17, 2024
Version 1.0.0

Presented by 0xMacro

Table of Contents

Introduction

This document includes the results of the security audit for Cannon's smart contract code as found in the section titled ‘Source Code’. The security audit was performed by the Macro security team on June 3rdth to June 4th 2024.

The purpose of this audit is to review the source code of certain Cannon Solidity contracts, and provide feedback on the design, architecture, and quality of the source code with an emphasis on validating the correctness and security of the software in its entirety.

Disclaimer: While Macro’s review is comprehensive and has surfaced some changes that should be made to the source code, this audit should not solely be relied upon for security, as no single audit is guaranteed to catch all possible bugs.

Overall Assessment

The following is an aggregation of issues found by the Macro Audit team:

Severity	Count	Acknowledged	Won't Do	Addressed
Low	1	-	-	1

Cannon was quick to respond to these issues.

Specification

Our understanding of the specification was based on the following sources:

- Discussions with the Cannon team.
- Available documentation in the repository.

Trust Model, Assumptions, and Accepted Risks (TMAAR)

Trusted Entities:

- Registry Owner: Has permission to upgrade the contract, and can set the publishing and registering fees.
- Package owner:

  When a package is registered an owner is set that can publish, unpublish, set publishers, and nominate a new owner, on ETH mainnet.

- Publishers:

  Set by the owner of the package, and can have different publishers on mainnet or optimism. Have the ability to publish and unpublish on the package they have

privileges for.

Source Code

The following source code was reviewed during the audit:

- **Repository:** cannon
- **Commit Hash:** `3e60f39e7b3320f45fd62e8fc7f43ebf8cdf420d`

Specifically, we audited the following contracts within this repository.

Contract	SHA256
contracts/CannonRegistry.sol	`f93d5aa728bb40e889b0b2a39b7c896e4435af4d29103ccabce7ffde57d1918c`
contracts/ERC2771Context.sol	`0092739f1e08cfa33029b2605181f708c933ae8dada0fd876da324f2ffeadc66`
contracts/EfficientStorage.sol	`f47a3769038c228370c2b21d23f8100bff76f685259d707dd15d856133b28206`
contracts/OwnedUpgradable.sol	`02be9afe23cb5cdc8a1a313fe8ad7cfe7cf95292c566d3e66e662910781cc001`
contracts/Proxy.sol	`f598ee07848d61daca27fe2fd0e17c764720251f228368a007aa1ee748da98bc`

Note: This document contains an audit solely of the Solidity contracts listed above. Specifically, the audit pertains only to the contracts themselves, and does not pertain to any other programs or scripts, including deployment scripts.

Issue Descriptions and Recommendations

Click on an issue to jump to it, or scroll down to see them all.

 Invalid package names can be accepted

Security Level Reference

We quantify issues in three parts:

1. The high/medium/low/spec-breaking **impact** of the issue:
    - How bad things can get (for a vulnerability)
    - The significance of an improvement (for a code quality issue)
    - The amount of gas saved (for a gas optimization)
2. The high/medium/low **likelihood** of the issue:
    - How likely is the issue to occur (for a vulnerability)
3. The overall critical/high/medium/low **severity** of the issue.

This third part – the severity level – is a summary of how much consideration the client should give to fixing the issue. We assign severity according to the table of guidelines below:

Severity	Description
(C-x) Critical	We recommend the client **must** fix the issue, no matter what, because not fixing would mean **significant funds/assets WILL be lost.**
(H-x) High	We recommend the client **must** address the issue, no matter what, because not fixing would be very bad, *or* some funds/assets will be lost, *or* the code's behavior is against the provided spec.
(M-x) Medium	We recommend the client to **seriously consider** fixing the issue, as the implications of not fixing the issue are severe enough to impact the project significantly, albiet not in an existential manner.
(L-x) Low	The risk is small, unlikely, or may not relevant to the project in a meaningful way. Whether or not the project wants to develop a fix is up to the goals and needs of the project.
(Q-x) Code Quality	The issue identified does not pose any obvious risk, but fixing could improve overall code quality, on-chain composability, developer ergonomics, or even certain aspects of protocol design.
(I-x) Informational	Warnings and things to keep in mind when operating the protocol. No immediate action required.
(G-x) Gas Optimizations	The presented optimization suggestion would save an amount of gas significant enough, in our opinion, to be worth the development cost of implementing it.

Issue Details

~~L-1~~ Invalid package names can be accepted

TOPIC	STATUS	IMPACT	LIKELIHOOD
Input validation	Fixed	Low	Low

When registering a package, via `setPackageOwnership()` the package name is validated to have expected characters and a set format:

```
/**
 * @notice Determines if the given _name can be used to register a package
 * @param _name the string to check if its a valid package name for registratic
 */
function validatePackageName(bytes32 _name) public pure returns (bool) {
  // each character must be in the supported charset

  for (uint256 i = 0; i < 32; i++) {
    if (_name[i] == bytes1(0)) {
      // must be long enough
      if (i < MIN_PACKAGE_NAME_LENGTH) {
        return false;
      }

      // last character cannot be `-`
      if (_name[i - 1] == "-") {
        return false;
      }

      break;
    }

    // must be in valid character set
    if (
      (_name[i] < "0" || _name[i] > "9") &&
          (_name[i] < "a" || _name[i] > "z") &&
```

```
          // first character cannot be `-`
          (i == 0 || _name[i] != "-")
        ) {
          return false;
        }
      }

      return true;
    }
```

Reference: CannonRegistry.sol#L410-L444

This will accept a package name with up to 32 characters, with a limited character set, and some exceptions. Cannon scripts take in a string value for the name, and convert it to a bytes32 value. In doing so, it only accepts strings with less than 32 characters to it can insert a null terminator character at the end. In the case where a package is registered directly, or outside cannon, inputting a package name of length 32, and without a null terminator, then cannon will currently fail to be able to use this package name in its scripts.

Remediations to Consider

Either adjust cannon to handle 32 character strings with no null terminator, or explicitly require the last character is `bytes(0)` in `validatePackageName()` to ensure all package names work as expected.

Disclaimer

Macro makes no warranties, either express, implied, statutory, or otherwise, with respect to the services or deliverables provided in this report, and Macro specifically disclaims all implied warranties of merchantability, fitness for a particular purpose, noninfringement and those arising from a course of dealing, usage or trade with respect thereto, and all such warranties are hereby excluded to the fullest extent permitted by law.

Macro will not be liable for any lost profits, business, contracts, revenue, goodwill, production, anticipated savings, loss of data, or costs of procurement of substitute goods or services or for any claim or demand by any other party. In no event will Macro be liable for consequential, incidental, special, indirect, or exemplary damages arising out of this agreement or any work statement, however caused and (to the fullest extent permitted by law) under any theory of liability (including negligence), even if Macro has been advised of the possibility of such damages.

The scope of this report and review is limited to a review of only the code presented by the Cannon team and only the source code Macro notes as being within the scope of Macro's review within this report. This report does not include an audit of the deployment scripts used to deploy the Solidity contracts in the repository corresponding to this audit. Specifically, for the avoidance of doubt, this report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project. In this report you may through hypertext or other computer links, gain access to websites operated by persons other than Macro. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such websites' owners. You agree that Macro is not responsible for the content or operation of such websites, and that Macro shall have no liability to your or any other person or entity for the use of third party websites. Macro assumes no responsibility for the use of third party software and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.