EVM CCTP

Public Security Assessment

December 19th, 2024 — Prepared by OtterSec

Robert Chen r@osec.io

Nicholas R. Putra nicholas@osec.io

Renato Eugenio Maria Marziano renato@osec.io

Table of Contents

Appendices

01 — Executive Summary

Overview

Circlefin engaged OtterSec to assess the `cctp-v2` program. This assessment was conducted between December 6th and December 17th, 2024. For more information on our auditing methodology, refer to Appendix B.

Key Findings

We produced 1 suggestion throughout this audit engagement.

We recommend ensuring that the code implementation aligns with the specifications for consistency (OS-ECP-SUG-00).

Scope

The source code was delivered to us in a Git repository at https://github.com/circlefin/evm-cctp-contracts-private. This audit was performed against 5ee9bbd up to 7d70310.

A brief description of the program is as follows:

Name	Description
cctp-v2	It describes the version 2 (v2) of the cross-chain transfer protocol, which enables token minting based on burns occurring on a different domain (chain), ensuring a 1:1 equivalence between tokens across domains.

02 — General Findings

Here, we present a discussion of general findings during our audit. While these findings do not present an immediate security impact, they represent anti-patterns and may result in security issues in the future.

ID	Description
OS-ECP-SUG-00	There are multiple inconsistencies between the specification and the implementation of the code.

Inconsistency in Specification and Implementation OS-ECP-SUG-00

Description

There are multiple inconsistencies in the specification documentation. Below are the list of the inconcistencies:

1. The `receiveMessage` event does not include the emission of the `minFinalityThresholdRequested` field.

>_ src/v2/MessageTransmitterV2.sol SOLIDITY

```
function receiveMessage(
    bytes calldata message,
    bytes calldata attestation
) external override whenNotPaused returns (bool success) {
    [...]

    // Emit MessageReceived event
    emit MessageReceived(
        msg.sender,
        _sourceDomain,
        _nonce,
        _sender,
        _finalityThresholdExecuted,
        _messageBody
    );

    return true;
}
```

2. The `depositForBurn` does not return the `nonce` in the current implementation.

>_ src/v2/TokenMessengerV2.sol SOLIDITY

```
function depositForBurn(
    uint256 amount,
    uint32 destinationDomain,
    bytes32 mintRecipient,
    address burnToken,
    bytes32 destinationCaller,
    uint256 maxFee,
    uint32 minFinalityThreshold
) external notDenylistedCallers {
    bytes calldata _emptyHookData = msg.data[0:0];
    _depositForBurn(
        amount,
        destinationDomain,
```

```
            mintRecipient,
            burnToken,
            destinationCaller,
            maxFee,
            minFinalityThreshold,
            _emptyHookData
        );
    }
```

We suggest ensuring that the code implementation aligns with the specifications for consistency.

Remediation

Implement the above-mentioned suggestion.

A — Vulnerability Rating Scale

We rated our findings according to the following scale. Vulnerabilities have immediate security implications. Informational findings may be found in the General Findings.

CRITICAL

Vulnerabilities that immediately result in a loss of user funds with minimal preconditions.

Examples:

- Misconfigured authority or access control validation.
- Improperly designed economic incentives leading to loss of funds.

HIGH

Vulnerabilities that may result in a loss of user funds but are potentially difficult to exploit.

Examples:

- Loss of funds requiring specific victim interactions.
- Exploitation involving high capital requirement with respect to payout.

MEDIUM

Vulnerabilities that may result in denial of service scenarios or degraded usability.

Examples:

- Computational limit exhaustion through malicious input.
- Forced exceptions in the normal user flow.

LOW

Low probability vulnerabilities, which are still exploitable but require extenuating circumstances or undue risk.

Examples:

- Oracle manipulation with large capital requirements and multiple transactions.

INFO

Best practices to mitigate future security risks. These are classified as general findings.

Examples:

- Explicit assertion of critical internal invariants.
- Improved input validation.

B — Procedure

As part of our standard auditing procedure, we split our analysis into two main sections: design and implementation.

When auditing the design of a program, we aim to ensure that the overall economic architecture is sound in the context of an on-chain program. In other words, there is no way to steal funds or deny service, ignoring any chain-specific quirks. This usually requires a deep understanding of the program's internal interactions, potential game theory implications, and general on-chain execution primitives.

One example of a design vulnerability would be an on-chain oracle that could be manipulated by flash loans or large deposits. Such a design would generally be unsound regardless of which chain the oracle is deployed on.

On the other hand, auditing the program's implementation requires a deep understanding of the chain's execution model. While this varies from chain to chain, some common implementation vulnerabilities include reentrancy, account ownership issues, arithmetic overflows, and rounding bugs.

As a general rule of thumb, implementation vulnerabilities tend to be more "checklist" style. In contrast, design vulnerabilities require a strong understanding of the underlying system and the various interactions: both with the user and cross-program.

As we approach any new target, we strive to comprehensively understand the program first. In our audits, we always approach targets with a team of auditors. This allows us to share thoughts and collaborate, picking up on details that others may have missed.

While sometimes the line between design and implementation can be blurry, we hope this gives some insight into our auditing procedure and thought process.