NCC Group
650 California St, Suite 2950
San Francisco, CA 94108
415.268.9300
https://nccgroup.com/us

Onomy Protocol

April 23, 2021

Introduction

In April 2021, Onomy engaged NCC Group to conduct a security assessment of the NOM smart contracts, designed to implement a token distribution using an Ethereum smart contract which uses a bonding curve strategy. Two consultants spent a total of 6 person-days reviewing the contracts for security flaws. Source code was provided, and the assessment was conducted through a combination of manual source code review and dynamic analysis. The purpose of this assessment was to identify smart-contract security issues that could adversely affect Ononmy. This assessment was performed by NCC Group under the guidelines provided in the statement of work for the engagement.

Detailed Letter of Engagement Overview

NCC Group is a global information assurance firm that, in the US, specializes in application, mobile, network, host, and product security. Security conscious companies use NCC Group's Detailed Letters of Engagement to verify product attributes in view of current security best practices, standard security functionality, and product protection. More information about the Group's processes and products can be found at https://nccgroup.com/us.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This Detailed Letter of Engagement necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. Any mention of effort or length of engagement is not intended to convey coverage; specifically, NCC Group makes no claim of complete coverage of the target(s) of this document. The information presented here should not be construed as professional advice or service.

Testing Methods

Testing was performed using a white-box methodology. NCC Group's consultants used a combination of manual test techniques and proprietary and public automated tools throughout the assessment. Onomy's smart contract was reviewed for

- Identity dangerous code paths using manual review and automated analysis tools
- Evaluate security impact when encountering exceptional or unintended code paths, including multi-contract scenarios, gasless spend, or exhausted call stack
- Evaluate state management within the contract, including proper transition during successful and unsuccessful function calls
- Evaluate time-related functions and ensuring that an attacker is unable to gain an advantage
- Verification of precision for the fixed point math
- Ensure that smart contract is not susceptible to common smart contract vulnerabilities such as described on the Decentralized Application Security Project (http://dasp.co/)
- Smart Contract Attacker Analysis: NCC Group will identify threats to the contract and associated risks, such as ways for an attacker to:
  - Compel execution of unintended code
  - Bypass contract logic or validation routines
  - Transfer assets without proper authorization

  - Compromise critical operations

Summary of Findings

Onomy effectively supported the test process, providing source code access and key developers to answer any questions the testing team had. During the assessment, NCC Group identified:

- One (1) high finding
- One (1) medium finding
- Two (2) low findings
- Three (3) informational findings

After the retest, NCC identified the following which marked as "Risk Accepted"

- Two (2) low findings
- Two (2) informational finding

Additionally, the following was marked as "Fixed" due to a code change, but the broader recommendations around testing are considered "Risk Accepted"

- One (1) informational finding

Upon completion of the assessment, all findings were reported to Onomy, along with recommendations.