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

August 5, 2022

Meta Platforms, Inc.
One Hacker Way
Menlo Park, CA 94025 USA

Introduction

Between the days of May 16th and May 20th, 2022, two (2) consultants from NCC Group engaged in a security test for a total of ten (10) person-days of effort reviewing Meta Platforms, Inc.'s Multi-Key Private-ID implementation.

The purpose of this assessment was to identify application-level security issues that could adversely affect the security of the Multi-Key Private-ID implementation. 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. The information presented here should not be construed as professional advice or service.

Testing Methods

Testing was performed using NCC Group's standard methodology for a Cryptography Services security assessment. Meta Platforms, Inc. provided NCC Group with access to source code and documentation in order to improve the effectiveness of the testing. NCC Group's consultants used a combination of manual test techniques and public automated tools throughout the assessment. The following aspects of the Multi-Key Private-ID implementation were reviewed as part of this assessment:

- Appropriate use of cryptographic primitives
- Appropriate invocations of cryptographic APIs and handling of error cases
- Identification of memory safety issues
- Review of side channels in cryptographic primitives and protocols
- Detailed review of deviations from the Multi-key Private-ID Reference Paper
- Analysis of cryptographic protocol sequences and data flows

Summary of Findings

During the assessment, NCC Group identified:

- One (1) medium severity vulnerability
- Two (2) low severity vulnerabilities
- One (1) informational finding

Upon completion of the assessment, all findings were reported to Meta Platforms, Inc. along with recommendations.

Between the dates of August 3rd and August 4th, 2022, NCC Group retested these vulnerabilities in accordance with the above methodology and observed that the following issues remained open:

- Two (2) low severity vulnerabilities

One was partially fixed by Meta Platforms, Inc. but had some remaining open items. The second remains unfixed, its risk being accepted by the Meta Platforms, Inc. team.