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

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

February 11, 2022

Introduction

Between the days of January 31st and February 11th, 2022, three (3) consultants from NCC Group, including one shadow resource, engaged in a Cryptography Services security assessment for a total of twenty (20) person-days of effort to assess the security of changes to the third-party EMP Toolkit library used by Meta Platforms, Inc. NCC Group previously performed a security assessment of EMP Toolkit for Meta Platforms, Inc. in September 2020. The changes examined in the current review included fixes to address vulnerabilities previously identified by NCC Group, as well as the addition of new cryptographic primitives and expanded functionality.

The purpose of this assessment was to identify application-level security and cryptography issues that could adversely affect the security of the EMP Toolkit and its use by Meta Platforms, Inc. in its Private Measurement applications. 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 NCC Group's standard methodology for a Cryptography Services security assessment. Meta Platforms, Inc. provided NCC Group with pointers to specific versions of the `emp-tool`, `emp-ot`, and `emp-sh2pc` code used in order to improve the effectiveness of the testing. NCC Group's consultants used a combination of manual test techniques and proprietary and public automated tools throughout the assessment. The following activities were carried out as part of this assessment:

- Review fixes to previously identified findings, including:
  - Potential uses of non-random data
  - Handling of potential failure of seeding pseudo-random number generators
  - Effectiveness of parameter validation
- Analysis of implementation of cryptographic primitives
- Analysis of planned use cases and assurances desired of the cryptosystem in comparison to the specific cryptographic primitives used
- Identification of threats to the cryptosystem and the risks associated with threats

- Identification of memory safety issues

Summary of Findings

Meta Platforms, Inc. effectively supported the test process. NCC Group retested vulnerabilities from the previous review in September 2020 and observed that the following issues remained open:

- Zero (0) high severity vulnerabilities
- Zero (0) medium severity vulnerabilities
- Two (2) low severity vulnerabilities

During the assessment, NCC Group identified no new findings in the changes to EMP Toolkit.