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

June 27, 2022

Introduction

Between the days of January 17th and January 28th, 2022, two (2) consultants from NCC Group engaged in a Cryptography Services security assessment for a total of twenty (20) person-days of effort reviewing Meta Platforms, Inc.'s Write-only Oblivious RAM (ORAM).

The purpose of this assessment was to identify application-level security and cryptography issues that could adversely affect the security of the Write-only ORAM application. This assessment was performed by NCC Group under the guidelines provided in the statement of work for the engagement.

On June 16th and 17th, 2022, two (2) consultants from NCC Group spent a further three (3) person-days of effort reviewing changes made to the Write-only ORAM application by Meta Platforms, Inc. in response to the January 2022 security assessment.

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 proprietary and public automated tools throughout the assessment. The following aspects of Write-only ORAM were reviewed as part of this assessment:

- Review of functional and design documentation describing the use of cryptography, with emphasis on security and functional requirements of the system
- Analysis of planned use cases and assurances desired of the cryptosystem in comparison to the design documents and libraries in use
- Identification of threats to the cryptosystem and the risks associated with threats
- Analysis of cryptographic protocol sequences and data flows
- Review of side channels in cryptographic primitives and protocols
- Analysis of implementation of cryptographic primitives

Summary of Findings

During the assessment, NCC Group identified:

- Zero (0) high severity vulnerabilities
- Zero (0) medium severity vulnerabilities
- 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 June 16th and June 17th, 2022, NCC Group retested these vulnerabilities in accordance with the above methodology and observed that no issues remained open.

Prepared by NCC Group Security Services, Inc. for Meta Platforms, Inc.. Portions of this document and the templates used in its production are the property of NCC Group and cannot be copied (in full or in part) without NCC Group's permission. While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group's services does not guarantee the security of a system, or that computer intrusions will not occur.