RIPE NCC Response to the Penetration Test Report from Radically Open Security

RIPE NCC RESPONSE TO THE PENETRATION TEST REPORT FROM RADICALLY OPEN SECURITY 1

1. Executive Summary 2

1.1 Introduction 2

1.2 Scope 2

1.3 Project Objectives 2

1.4 Timeline 2

1.5 Results in a nutshell 2

1.6 Summary of findings 2

1.7 Summary of recommendations 3

2. Methodology 3

3. Reconnaissance and Fingerprinting 3

4. Findings 3

4.1 RIPE-009 - Unencrypted Communication 3

4.2 RIPE-008 - Cross Site Request Forgery 3

4.3 RIPE-007 4

4.4 RIPE-006 4

4.5 RIPE-005 4

4.6 RIPE-004 - Improper input validation 4

4.7 RIPE-003 5

4.8 RIPE-001 5

5 Non-Findings 5

5.1 NF-002 5

1. Executive Summary

1.1 Introduction

Every year we ask an external party to carry out a security audit of our RPKI systems. We publish the security report in an effort to increase transparency and trust in the RPKI system. In this report, we list the findings of the external party that carried out this penetration test and how we mitigated these issues.

Between 23 June and 22 July 2021, Radically Open Security B.V. (ROS) carried out a penetration test and code review for the RIPE NCC. These audits were intended to assess the security level of the various components of RPKI. We are committed to having annual security assessments and sharing the findings when appropriate.

1.2 Scope

The scope of the penetration test included the externally (and transitively) accessible systems from a user perspective, with a focus on the RPKI functionality. Among others, this included:

- my.ripe.net
- lirportal.ripe.net
- access.ripe.net

1.3 Project Objectives

The project objectives are described in the report from ROS.

1.4 Timeline

This penetration test took place between 23 June and 22 July 2021.

1.5 Results in a Nutshell

During this white-box penetration test, ROS found three elevated, four moderate and one low-severity issue. These details are described in detail in section 4 of the ROS report.

1.6 Summary of findings

The summary of findings are described in the report from ROS.

1.7 Summary of recommendations

The summary of recommendations are described in the report from ROS.

2. Methodology

This section in the ROS report describes the methodology and risk classifications used for the penetration test.

3. Reconnaissance and Fingerprinting

This section in the ROS report describes the different automated scans used for the penetration test.

4. Findings

4.1 RIPE-009 - Unencrypted Communication

Vulnerability type: Transport Layer Security
Threat Level: Elevated

ROS: The applications at https://ba-apps.prepdev.ripe.net and http://core-1.rpki.prepdev.ripe.net:8080 work over HTTP, which is an unencrypted medium.

RIPE NCC: We changed RPKI core and ba-apps to only be available over HTTPS so that all traffic is encrypted. Up-down remains on HTTP and uses a CMS wrapper for authentication. Switching up-down to HTTPS is not possible without user impact. This would require delegated CAs and using an implementation that does not follow redirects, to reconfigure their CA.

4.2 RIPE-008 - Cross Site Request Forgery

Vulnerability type: CSRF
Threat level: Moderate

ROS: The application at https://lirportal.prepdev.ripe.net/ does not implement anti-CSRF controls on some of its endpoints.

RIPE NCC: We have implemented CSRF protection.

4.3 RIPE-007

Vulnerability type: Session management
Threat level: Low

ROS: The https://lirportal.prepdev.ripe.net/training/ endpoint requires the JSESSIONID cookie only, which does not expire on user logout. Moreover, the cookie is missing its secure flag.

RIPE NCC: We have fixed the expiration of the JSESSIONID token on logout. Moreover, we have set the secure flag on all cookies.

4.4 RIPE-006

Vulnerability type: Insecure configuration
Threat level: Elevated

ROS: The endpoint https://my.prepdev.ripe.net/api/file-attachment allows the uploading of all files, irrespective of file type. Also the endpoint does not implement any anti-automation.

RIPE NCC: We have implemented validation to allow a small set of file types to be uploaded through the RIPE portal. Limits are in place for a maximum file upload size. Also we monitor our systems for abuse and we can mitigate automated attacks by using a web application firewall.

4.5 RIPE-005

Vulnerability type: Authentication
Threat level: Moderate

ROS: A password reset link sent to a user’s email address is not invalidated if the user’s registered email is changed afterwards.

RIPE NCC: We have fixed this so that on changing a user’s email address any pending password reset link is invalidated.

4.6 RIPE-004 - Improper input validation

Vulnerability type: Improper input validation
Threat level: Moderate

ROS: The application uses the user-submitted value of the JSON parameter and copies it into the HTML document as plain text between tags.

RIPE NCC: We now properly validate user-submitted values and encode those where necessary. All responses on the API endpoints now return a relevant Content-Type.

4.7 RIPE-003

Vulnerability type: Open redirect
Threat level: Elevated

ROS: The endpoint https://access.prepdev.ripe.net/?originalUrl= allows redirection to any ripe.net subdomain.

RIPE NCC: We have restricted the redirect to https urls of allowed subdomains of ripe.net.

4.8 RIPE-001

Vulnerability type: Insecure configuration
Threat level: Moderate

ROS: The HTML5 cross-origin resource sharing (CORS) policy for the request to endpoint https://access.prepdev.ripe.net/user/profile allows access from any domain.

RIPE NCC: We have fixed the CORS policy and strictly validate whether the origin is allowed and is on a subdomain of ripe.net.

5 Non-Findings

This section of the ROS report describes attempts made that turned out to be dead ends.

5.1 NF-002

ROS: During the penetration test, we performed the following tests which did not result in any vulnerability.

RIPE NCC: The fairly elaborate list of test cases did not lead to any findings, which is a good sign.