

RPost US Inc.
6033 W. Century Blvd.
Ste. 1278
Los Angeles, CA 90045

March 26, 2020

To: Tim Jenks
VP of Technology
RPost US Inc.

RE: Google Project ID: 456065093154

From January 22, 2020 through January 31, 2020, Leviathan Security Group conducted a limited penetration test and document review of the RPost application produced by RPost US, Inc. We assessed the application, supporting infrastructure, and RPost US, Inc.'s answers in a self-assessment questionnaire.

Leviathan verified the application's use of the following **restricted** Google API scope:

<https://mail.google.com>

RPost US, Inc.'s Vulnerability Disclosure policy can be found at <https://support.rpost.com/hc/en-us/articles/360043708773-Vulnerability-Disclosure-Policy-Vulnerability-Report-Submission>. Reports are made via e-mail to support@rpost.com. This e-mail address is monitored by the Security Team.

This testing was undertaken as a part of the Google Cloud Platform OAuth API Verification and should not be read as a comprehensive penetration test or maturity assessment. The purpose of the engagement was to identify security issues with RPost US, Inc.'s application and infrastructure during the time allocated to us. Leviathan used automated and manual testing as well as review of the Self-Assessment Questionnaire filled out by RPost US, Inc. and associated documentation.

This letter confirms that the testing of the RPost application and supporting infrastructure has been completed and that all issues with a Critical or High-risk finding have been remediated. RPost US, Inc.'s management has received a report with detailed findings and recommendations from this engagement.

The testing followed the requirements as described in the OAuth API Verification FAQ as last updated on November 4, 2019. These requirements are detailed in Appendix A at the end of this letter. This letter is valid for up to 12 months from the issue date.

Signed,



Bob Bregant
Director, Risk and Advisory Services
Leviathan Security Group

Appendix A

1. *External Network Penetration Testing: Identify potential vulnerabilities in external, internet-facing infrastructure, systems such as the following:*
 - *Discovery and enumeration of live hosts, open ports, services, unpatched software, administration interfaces, authentication endpoints lacking MFA, and other external-facing assets*
 - *Automated vulnerability scanning combined with manual validation*
 - *Brute-forcing of authentication endpoints, directory listings, and other external assets*
 - *Analysis of potential vulnerabilities to validate and develop complex attack chaining patterns and custom exploits*
 - *Potential exploitation of software vulnerabilities, insecure configurations, and design flaws*
2. *Application Penetration Testing: Identify potential vulnerabilities in application that access Google user data such as the following:*
 - *Real-world attack simulation focused on identification and exploitation*
 - *Discovery of attack surface, authorization bypass, and input validation issues*
 - *Automated vulnerability scanning combined with manual validation*
 - *Exploitation of software vulnerabilities, insecure configurations, design flaws, and weak authentication*
 - *Analysis of vulnerabilities to validate and develop complex attack chaining patterns and custom exploits*
 - *Verify the ability for users to delete their account with no external indication that the user or user's content is accessible.*
3. *Deployment Review: Identify exploits and vulnerabilities in developer infrastructure such as the following:*
 - *Gathering all available configuration settings and metadata as well as manual techniques to build a profile of the cloud environment*
 - *Analyzing collected information to identify any gaps or deviations from accepted cloud security best practices*
 - *Manually examining configuration settings to locate anomalies and issues such as weak IAM policies, exposed storage containers, poorly defined security groups, insecure cloud services usage, and insecure key management*
 - *Exploitation of vulnerabilities, insecure configurations, design flaws, and weak authentication – as needed*
 - *Verify storage of OAuth tokens is encrypted and encryption keys and secrets are stored in a hardware security module or equivalent strength key manager*
 - *Ensure developer access to the deployment environment is secured with multi-factor authentication*
4. *Policy and Procedure Review: Review and examine the efficacy of information security policies and procedures such as the following:*
 - *Incident Response Plan: Establishes roles, responsibilities, and actions when an incident occurs*

- *Risk Management Policy: Identifies, reduces, and prevents undesirable incidents or outcomes*
- *Vulnerability Disclosure Program: Provides a means for external parties to report vulnerabilities*
- *Information Security Policy: Ensures that all users comply with rules and guidelines related to the security of the information stored digitally at any point in the network*
- *Privacy User Data Detection: Ensures that users can delete their accounts and related user data by demonstrating an account deletion if relevant*