Vulnerability Disclosure Policy

Postal Regulatory Commission

March 2, 2021

Introduction

The Postal Regulatory Commission (PRC) is committed to maintaining the security of its systems and protecting sensitive information from unauthorized disclosure. This Vulnerability Disclosure Policy outlines the systems and types of security research covered under this policy, guidelines for sending vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

The PRC encourages you to contact us to report potential vulnerabilities in its systems.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized and we will work with you to understand and resolve the issue quickly, and the *PRC* will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Guidelines

Security researchers shall:

- Notify the PRC as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid degradation of user experience, disruption to production systems, destruction or manipulation of data and ensure privacy violations do not occur.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to pivot to other systems.
- Keep confidential any information about discovered vulnerabilities for up to 180 calendar days after you have notified PRC and received confirmation of receipt.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, non-public, proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Test methods

Security researchers must not:

- Test any system other than the systems set forth in the ‘Scope’ section below

- Conduct Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Conduct Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing
- Conduct Brute force attempts of passwords, directories or resource discovery
- Introduce malicious software
- Test third-party applications, websites, or services that integrate with or link to or from PRC systems
- Delete, alter, share, retain, or destroy PRC data, or render PRC data inaccessible, or, use an exploit to exfiltrate data, establish command line access, establish a persistent presence on PRC systems, or “pivot” to other PRC systems

Scope

This policy applies to the following systems and services:

prc.gov

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy’s scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren’t sure whether a system is in scope or not, contact us at itsecure@prc.gov before starting your research (or at the security contact for the system’s domain name listed in the .gov WHOIS).

Though we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first.

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only - to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely PRC, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We accept vulnerability reports at itsecure@prc.gov. Acceptable message formats are plain text, rich text, and HTML. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days. We do not support PGP-encrypted emails.

By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against the U.S. Government related to your submission. The PRC does not operate a bug bounty program.

What we would like to see from you

In order to help the PRC triage and prioritize submissions, we recommend that your reports:

- Describe the type of issue, the location of the vulnerability was discovered and the potential impact of exploitation
- Offer a detailed, step-by-step description of the process needed to reproduce the vulnerability, including a description of any tools needed to identify or exploit the vulnerability (proof-of-concept scripts or screenshots are helpful)
- Any technical information and related materials we would need to reproduce the issue
- Suggested mitigation or remediation actions, as appropriate
- Be in English, if possible

What you can expect from us

When you choose to share your contact information with the PRC, the PRC commits to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received.
- To the best of the PRC's ability, we will confirm the existence of the vulnerability and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will be open to continued dialogue to discuss the issue.

Questions

Questions regarding this policy may be sent to **itsecure@prc.gov**. The PRC also invites you to contact us with suggestions for improving this policy.

Document change history

Version	**Date**	**Description**
1.0	*March 2, 2021*	First issuance.