External Vulnerability Disclosure Policy

PROS Information Security Program

Version 1.2

Data Classification: Public

2025

1. Purpose

PROS is committed to maintaining the highest standards of security for our software products and services. This External Vulnerability Disclosure Policy outlines how security researchers, ethical hackers, and external parties can responsibly report vulnerabilities they discover in our systems, ensuring the safety and integrity of our products and the trust of our users.

2. Scope

This policy applies to all external parties (researchers, ethical hackers, and other stakeholders) who identify and report vulnerabilities in PROS software products, services, websites, and related infrastructure. It covers all forms of vulnerabilities, including but not limited to:

- Software applications (web, mobile, desktop)
- APIs and web services
- Cloud infrastructure
- Network services
- Documentation and public-facing resources

Excluded: This policy does not apply to vulnerabilities discovered in internal systems or any non-publicly accessible systems unless explicitly authorized by PROS.

3. Definitions

- **Vulnerability:** A weakness in the system that can be exploited to compromise the confidentiality, integrity, or availability of the system or its data.
- **Responsible Disclosure:** The practice of privately reporting security vulnerabilities to the affected organization, allowing them time to address the issue before public disclosure.
- **Safe Harbor:** Legal protections provided to individuals who report vulnerabilities in good faith, preventing legal action by PROS as long as the reporting adheres to the policy.

4. Policy Statements

4.1. Encouragement of Responsible Disclosure

PROS encourages security researchers and external parties to report vulnerabilities responsibly. We value the contributions of the security community in enhancing the security of our products and services.

4.2. Legal Safe Harbor

To protect individuals who report vulnerabilities in good faith, PROS offers safe harbor provisions. As long as the reporter:

- Engages in responsible and ethical behavior.
- Does not perform unauthorized testing or actions beyond what is necessary to discover the vulnerability.
- Adheres to the guidelines outlined in this policy.

then PROS will not initiate legal action against them.

4.3. No Authorization to Access

This policy does not grant permission to conduct security testing or access systems beyond what is necessary to identify and report the vulnerability. Unauthorized access or testing may violate applicable laws.

5. Reporting Process

5.1. How to Report a Vulnerability

Vulnerabilities can be reported through the following channels:

- **Email:** security@pros.com

5.2. Required Information

When reporting a vulnerability, please include the following information to facilitate timely assessment and remediation:

- **Contact Information:** Your name, email address, and any other relevant contact details.
- **Description:** A clear and detailed description of the vulnerability.
- **Impact:** Potential impact and severity of the vulnerability.
- **Reproduction Steps:** Step-by-step instructions to reproduce the vulnerability.
- **Proof of Concept:** Any code snippets, screenshots, or other evidence demonstrating the vulnerability.
- **Affected Systems:** Specific products, services, or versions affected.

6. Response and Acknowledgment

6.1. Initial Acknowledgment

Upon receiving a vulnerability report, PROS will acknowledge receipt within [e.g., 5 business days]. The acknowledgment will include:

- Confirmation that the report has been received.
- A reference number for tracking.
- An estimated timeline for further communication.

6.2. Assessment and Remediation

PROS will:

- Assess the validity and severity of the reported vulnerability.
- Prioritize remediation based on the impact and risk.
- Inform the reporter any necessary progress or communicate at closure.

6.3. Final Communication

Once the vulnerability has been addressed, PROS will:

- Inform the reporter of the resolution.

- Provide details on the fix, if appropriate.
- Coordinate public disclosure (if applicable) in a mutually agreed timeframe.

7. Recognition and Rewards

PROS may offer recognition or rewards for valid vulnerability reports, depending on the severity and impact. Rewards may include:

- **Certificate of Recognition**

Note: Participation in a rewards program is voluntary and not a prerequisite for reporting vulnerabilities.

8. Responsible Disclosure Guidelines

To ensure responsible disclosure, reporters should adhere to the following guidelines:

- **Do Not Exploit:** Do not exploit the vulnerability beyond what is necessary to demonstrate its existence.
- **Do Not Disclose Publicly:** Refrain from publicly disclosing the vulnerability until the Company has had sufficient time to address it.
- **Respect Privacy:** Avoid accessing or exposing any user data or private information.
- **Minimal Impact Testing:** Conduct testing in a manner that does not disrupt services or affect other users.

9. Communication and Transparency

PROS is committed to transparent communication with the security community. Updates regarding major vulnerabilities and their resolutions will be shared through:

- **Security Advisories:** Detailed reports on identified vulnerabilities and fixes.
- **Blogs and Newsletters:** Information on security improvements and best practices.
- **Public Statements:** Announcements on significant security incidents and responses.

10. Responsibilities

10.1. Security Team

- Manage and coordinate the vulnerability reporting and remediation process.
- Communicate with reporters and internal stakeholders.
- Ensure timely and effective resolution of reported vulnerabilities.

10.2. Development Teams

- Address and remediate identified vulnerabilities.
- Implement security best practices in the development lifecycle.
- Collaborate with the Security Team to ensure comprehensive fixes.

10.3. Management

- Provide necessary resources and support for the Security Team.
- Promote a culture of security awareness and responsible disclosure.
- Ensure compliance with relevant laws and regulations.

11. Compliance and Legal Considerations

- **Applicable Laws:** Reporters must comply with all applicable local, national, and international laws when testing and reporting vulnerabilities.
- **Privacy:** PROS respects the privacy of all individuals and commits to protecting personal data.

12. Policy Updates

PROS reserves the right to modify this External Vulnerability Disclosure Policy at any time. Updates will be published in the contract center on pros.com and will take effect immediately upon posting. It is the responsibility of the security leadership to review the policy periodically for any changes.

13. Contact Information

For any questions or further assistance regarding this policy, please contact:

- **Email:** security@pros.com

Thank you for helping us maintain the security and integrity of PROS products and services. Your contributions are highly valued and appreciated.

Document History

Document Title	External Vulnerability Disclosure Policy
Status	Review
IA Classification	Public
Document Owner	Chief Information Security Officer
Version	1.2
Effective	
Authors	Anthony Ali
Reviewers	Christine Lambden, Director Info Sec & Compliance
Approvers	Susanne Senoff, CISO

Date	Author	Action	Version
10/20/2024	Anthony Ali	Original draft	1.0
3/17/2025	Anthony Ali	Changes to Recognition and Rewards and Policy Update	1.1
3/18/2025	Christine Lambden	Convert to current policy template and assign classification	1.2