Proscia Coordinated Vulnerability Disclosure Policy

Overview

Proscia is committed to maintaining the security, safety, and reliability of its medical device software products and supporting cloud services. We recognize the important role that security researchers, customers, vendors, and other external parties play in identifying potential cybersecurity vulnerabilities.

Proscia encourages responsible reporting of security vulnerabilities so they can be evaluated and addressed in a timely and coordinated manner. This policy describes how potential vulnerabilities affecting Proscia products or services can be reported.

What Is a Security Vulnerability

A security vulnerability is an unintended weakness that could compromise the confidentiality, integrity, or availability of Proscia products, services, or data.

Examples may include weaknesses that could allow unauthorized access, modification of system behavior or data, disruption of service availability, or compromise of sensitive information.

Reporting a Vulnerability

If you believe you have identified a potential cybersecurity vulnerability affecting a Proscia product, service, or related infrastructure, please report the issue to:

support@proscia.com

When submitting a report, please include as much of the following information as possible:

- Product or service affected
- Software version or deployment configuration, if known
- Description of the vulnerability
- Steps required to reproduce the issue
- Potential impact of the vulnerability
- Supporting materials such as logs, screenshots, or proof-of-concept code if available

Providing detailed information will assist Proscia in investigating and resolving the reported issue.

© 2026 Proscia. All rights reserved.

Scope

This policy applies to vulnerabilities affecting systems, services, or software assets owned, operated, or maintained by Proscia, including:

- Proscia medical device software products
- Proscia-hosted cloud services supporting those products
- APIs and interfaces provided by Proscia
- software components and integrations maintained by Proscia

Issues affecting third-party products or services not controlled by Proscia should be reported directly to the applicable vendor.

Responsible Research Expectations

To protect patient safety, system availability, and data confidentiality, individuals reporting vulnerabilities are expected to:

- Conduct research and testing in a manner that does not negatively impact patient safety or clinical operations
- Avoid accessing, modifying, or exfiltrating patient data or other sensitive information
- Avoid disrupting production systems or degrading service availability
- Avoid automated scanning or testing that may impact system performance
- Coordinate vulnerability disclosure with Proscia prior to public release

Response and Investigation Process

Proscia will review all submitted vulnerability reports through its cybersecurity risk management process.

Proscia will:

- Acknowledge receipt of vulnerability reports within five (5) business days
- Review and investigate reported vulnerabilities
- Request additional information when needed to support investigation
- Implement remediation or mitigation actions when appropriate
- Coordinate public disclosure when applicable

Where public disclosure is appropriate, Proscia will coordinate disclosure timing with remediation availability when feasible and ensure consistency between public advisories and customer communications.

© 2026 Proscia. All rights reserved.

Good Faith Security Research

Proscia supports responsible security research and will not pursue legal action against individuals who report vulnerabilities in good faith and in accordance with this policy.

Security Advisories

When vulnerabilities require customer awareness or remediation actions, Proscia may communicate security advisories describing:

- affected product versions
- vulnerability severity
- remediation or mitigation guidance
- recommended actions for customers

Contact

All vulnerability reports and related questions should be directed to:

support@proscia.com

© 2026 Proscia. All rights reserved.