90 E Halsey Road
Suite 382
Parsippany, NJ 07054

inRangeSolutions.com
201.335.0090
973.860.2424

Security Vulnerability Disclosure Policy

inRange Solutions is committed to maintaining the security of its systems, products, and services, and to protecting the data of our customers, partners, and employees. We value the efforts of security researchers and the broader security community in helping us identify and address potential vulnerabilities. This policy outlines our guidelines for responsibly discovering and reporting security vulnerabilities.

Our Commitment

When you report a security vulnerability to us in accordance with this policy, we commit to:

- **Good Faith Engagement:** We will work with you in good faith to understand and resolve the reported issue.

- **Timely Review:** We will acknowledge receipt of your report within 5 business days and provide an estimated timeline for our initial review.

- **Investigation and Remediation:** We will investigate all legitimate reports and take appropriate action to remediate confirmed vulnerabilities.

- **Confidentiality:** We will maintain the confidentiality of your identity, if requested, to the extent legally permissible.

- **No Legal Action:** We will not pursue legal action against individuals who discover and report vulnerabilities in good faith and adhere to this policy.

Scope

This policy applies to security vulnerabilities found in:

- **inRange Solution's** corporate websites and web applications.

- **inRange Solution's** proprietary software and hardware products.

- Services directly operated by **inRange Solution**.

- Any other systems, applications, or services explicitly owned and operated by **inRange Solution**.

Vulnerabilities must be original, previously unreported, and directly impact the confidentiality, integrity, or availability of our systems, services, or data.

Out of Scope

The following activities are considered out of scope and are not authorized under this policy:

- **Social Engineering:** Any attempts to phish, trick, or otherwise manipulate **inRange Solutions** employees or contractors.
- **Physical Attacks:** Attempts to gain physical access to **inRange Solutions** facilities or equipment.
- **Denial of Service (DoS/DDoS) Attacks:** Any actions that could disrupt or degrade our services.
- **Automated Scanning:** Excessive automated scanning that could impact system performance or generate large volumes of irrelevant alerts.
- **Vulnerabilities in Third-Party Products/Services:** Issues in products or services not directly owned or controlled by **inRange Solutions** (please report these directly to the respective vendor).
- **Disclosure of Personally Identifiable Information (PII):** Accessing, modifying, or disclosing any customer, partner, or employee data.
- **Testing on Live Customer Data:** Any testing that involves accessing or manipulating live customer data.

Guidelines for Responsible Disclosure

We ask that security researchers adhere to the following guidelines:

- **Avoid Disruption:** Make every effort to avoid disruption to production systems, destruction of data, and privacy violations during your testing.
- **Non-Exploitation:** Do not exploit any discovered vulnerability beyond what is necessary to prove its existence.
- **Minimal Access:** Access only the data necessary to demonstrate the vulnerability. Do not download, copy, or store any data.
- **Confidentiality:** Keep information about any vulnerabilities you've discovered confidential between yourself and **inRange Solutions** until we have had at least 90 days to investigate and resolve the issue. Public disclosure should only occur after mutual agreement.
- **Legal Compliance:** Conduct all research and reporting activities in compliance with all applicable laws and regulations.

Reporting a Vulnerability

If you believe you have discovered a security vulnerability, please report it to us as soon as possible via:

Email: support@inrange-llc.com

Your report should include:

- **A clear and concise description** of the vulnerability.
- **The affected systems, applications, or services.**
- **Detailed steps to reproduce the vulnerability** (ex- URLs, parameters, proof-of-concept code).
- **Any supporting documentation or screenshots** that can help us understand the issue.
- **Your contact information** (optional, but helpful for follow-up or any questions).

Our Process

1. **Submission:** Upon receiving your report, we will send an acknowledgment within 5 business days.
2. **Validation:** Our security team will review and validate the reported vulnerability.
3. **Remediation:** If confirmed, we will prioritize and work to remediate the vulnerability.
4. **Communication:** We will keep you informed of our progress and the resolution of the vulnerability.
5. **Public Disclosure (Optional):** Once the vulnerability is resolved, we may, with your consent, publicly acknowledge your contribution.

Limitations

inRange Solutions does not currently operate a public bug bounty program and does not offer monetary rewards for vulnerability submissions.

Policy Review

This policy is reviewed periodically and updated as needed to reflect changes in our operations, security posture, or industry best practices.