Vulnerability Disclosure Policy

1. Purpose

Leica Camera AG and its affiliated companies (collectively the “Leica Group”) are committed to maintaining the security of its products and services. We value the responsible efforts of security researchers, customers, partners, and other individuals who help identify cybersecurity vulnerabilities.
We currently do not operate a vulnerability reward or bug bounty program.
This Vulnerability Disclosure Policy describes how security vulnerabilities can be reported to us and how we coordinate the handling and disclosure of reported vulnerabilities in accordance with applicable cybersecurity requirements, including Regulation (EU) 2024/2847 (Cyber Resilience Act - "CRA"), where applicable, and recognized industry practices for coordinated vulnerability disclosure.

2. Scope

This Policy applies to the Leica Group in relation to products and services developed, manufactured, operated or supported by the respective Leica Group company. The Leica Group operates a central Product Security Incident Response Team (PSIRT) which acts as the central point of contact for vulnerability reports covered by this Policy. Reports received by the PSIRT will be assessed and, where necessary, forwarded to and coordinated with the Leica Group company responsible for the affected product or service. It also applies to vulnerabilities affecting third-party or open-source components incorporated into or used as part of Leica Group products or services. Where a reported vulnerability originates from such a component, Leica Group will assess the impact on the affected Leica Group product or service and, where appropriate, coordinate with the relevant supplier, developer, or maintainer. Vulnerabilities exclusively affecting products or services that are neither owned, developed, operated, nor supported by Leica Group should be reported directly to the responsible provider.

3. Reporting a Vulnerability

If you believe you have discovered a security vulnerability in one of our products or

Leica Camera AG
Am Leitz-Park 5, 35578 Wetzlar, Deutschland, T +49 6441 2080-0, info@leica-camera.com, www.leica-camera.com
AG mit Sitz in Wetzlar, Amtsgericht Wetzlar HRB 966, AR-Vorsitzender: Dr. Andreas Kaufmann
Vorstand: Andreas Voll (CEO), Michael Grimm (CFO), Dr. Ronny Fritsche (COTO)

services, please report it as soon as possible by email.
Email: psirt@leica-camera.com
We kindly ask you not to publicly disclose a reported vulnerability until Leica Group has had a reasonable opportunity to investigate and remediate or mitigate the issue. Leica Group will seek to coordinate the timing of any public disclosure with the reporter, taking into account the severity of the vulnerability, the availability and deployment of a remediation, the potential impact on users, and any applicable legal or regulatory obligations.

4. Information to Include
To help us investigate your report efficiently, please include as much of the following information as possible:

- Vulnerability title
- Product name and model
- Affected URL or service (where applicable) (optional)
- Software or firmware version
- Description of the vulnerability
- Potential security impact
- Weakness classification (e.g., CWE), if known (optional)
- Severity assessment (e.g., CVSS), if known (optional)
- Steps to reproduce the issue
- Supporting evidence (such as screenshots, logs, or proof of concept)
- Possible mitigation or recommendation (optional)
- Your contact information for follow-up questions (optional)
- Please avoid including personal data, confidential information, or data relating to third parties in your report unless this is strictly necessary to demonstrate the vulnerability. Where possible, redact or anonymize such information before submitting it.

5. Our Commitment

Upon receiving a vulnerability report, we will:

- Acknowledge receipt of your report within **5 business days**.
- Review and assess the reported vulnerability.
- Aim to complete the initial technical assessment within **10 business days**, were reasonably practicable.
- Contact you if additional information is required.
- Keep you informed of significant progress where appropriate.
- Notify you when our investigation has been completed and, where appropriate, when a remediation or mitigation is available.

Where a reported vulnerability affects third-party components or suppliers, additional coordination may be required, and resolution timelines may be extended. Vulnerabilities are prioritized based on their potential impact, severity, exploitability, and the affected products or services. Investigation and remediation timelines may vary depending on the complexity of the issue.

6. Responsible Security Research

We ask security researchers to:

- Act in good faith and limit any testing to what is reasonably necessary to identify and demonstrate a potential vulnerability.
- Avoid disrupting, degrading, or impairing Leica Group products, services, or infrastructure, including through denial-of-service or excessive-load testing.
- Avoid accessing, copying, modifying, or deleting data belonging to other users or third parties and stop testing if such access occurs beyond what is strictly necessary to demonstrate the vulnerability.
- Where possible, use your own accounts, devices, and data for testing, and protect information about the vulnerability from unauthorized disclosure while remediation is being coordinated.
- Do not use social engineering, phishing, credential stuffing, brute-force techniques, or establish persistence or otherwise maintain unauthorized

access after the vulnerability has been demonstrated. Comply with all applicable laws and regulations during your research.

- Please use only the minimum testing necessary to demonstrate the vulnerability and avoid any action that could cause harm to Leica Group, its customers, or third parties.

7. Safe Harbor

Each company of the Leica Group will not initiate legal action solely on the basis of security research conducted in good faith and in accordance with this Policy in relation to products or services for which that company of the Leica Group is responsible, provided that the researchers:

- Act in good faith and comply with this Vulnerability Disclosure Policy.
- Limit testing to what is reasonably necessary to identify and demonstrate the vulnerability.
- Avoid intentional harm to the Leica Group, its customers, or third parties.
- Do not use a vulnerability for personal gain, unauthorized access, data extraction, or any purpose beyond responsible security research.
- Cooperate with the Leica Group in coordinating disclosure of the vulnerability before making information public.

This Safe Harbor applies only to activities conducted in accordance with this policy and does not apply to activities that fall outside its scope or affect rights or claims of third parties.
Nothing in this policy limits mandatory legal or regulatory obligations.

8. Security Advisories

Where required or appropriate, Leica Group, or the relevant company within the Leica Group, will publish information about remediated vulnerabilities and available security updates on its Product Security webpage. Where immediate disclosure could create additional cybersecurity risks, publication may be delayed until users have had a reasonable opportunity to apply the relevant remediation.

Security Advisories:

https://leica-camera.com/product-security

9. Contact Information

For all security vulnerability reports and questions related to this policy, please contact:

Product Security Incident Response Team (PSIRT) : psirt@leica-camera.com

Thank you for helping us improve the security of our products and protect our customers through responsible vulnerability disclosure.