iris-GmbH Infrared & Intelligent Sensors
Schnellerstr. 1–5 | 12439 Berlin
Germany

Policy (PO)

Coordinated Disclosure of Security Vulnerabilities in Products

Version:	1.0
Effective as of:	01.09.2026
Confidentiality:	Public

Contact

Reporting portal:	https://www.iris-sensing.com/support/
Security Advisories:	https://www.iris-sensing.com/support/security-advisories/
Email:	informationsecurity@iris-sensing.com

Contents

1 Introduction and Purpose 2
2 Scope 2
3 Reporting a Vulnerability 3
4 How We Handle Your Report 3
4.1 Process Flow and Deadlines 3
4.2 Assessment 3
4.3 Coordinated Disclosure 4
4.4 Security Advisory 4
5 What We Expect from Reporters 5
6 What Reporters Can Expect From Us 5
7 Security Updates and Patches 6

1 Introduction and Purpose

iris-GmbH infrared & intelligent sensors (hereinafter referred to as “iris”) takes the security of its products and the protection of its customers very seriously. We are convinced that responsible collaboration with security researchers, customers, partners, and the public is an essential part of product security.

This document describes how vulnerabilities in iris products can be reported to us, what reporters can expect from us, and how we handle reported vulnerabilities. It supports the implementation of the requirements for handling vulnerabilities in accordance with Regulation (EU) 2024/2847 (Cyber Resilience Act), in particular Annex I, Part II.

Furthermore, the procedure described here is seamlessly integrated into our certified information security management system (ISMS) in accordance with ISO/IEC 27001 and into the secure product development process in accordance with IEC 62443-4-1.

2 Scope

This guideline applies to all products and services offered by iris , in particular:

- Sensor hardware and embedded firmware
- Accompanying software, configuration tools, and applications
- Cloud services operated in connection with iris products
- Documentation and configuration guides, to the extent they are security-relevant

This policy does **not** apply **to** vulnerabilities in standalone third-party products that are not part of an iris product or service.
Vulnerabilities in third-party components that are part of an iris product are addressed as part of our vulnerability handling process and, if necessary, coordinated with the respective manufacturer.

3 Reporting a Vulnerability

Vulnerabilities can be reported to us via the contact information provided above. To ensure efficient processing, please include the following information in your report:

- **Affected product** and product version
- Firmware or software **version**
- **Description of the vulnerability**—type of vulnerability, date of discovery, reproducibility, and any potential solutions
- **Source** – Origin of the discovery (e.g., incident, penetration tests, vulnerability scans)
- **Severity** – Description of the potential impact if exploited
- **Contact Information** – Name (or pseudonym) and contact for follow-up questions

4 How we handle your report

4.1 Process Flow and Deadlines

STEP	DEADLINE	DESCRIPTION
ACKNOWLEDGMENT OF RECEIPT	48 hours	You will receive a confirmation with a reference number (ticket ID)
TRIAGE AND INITIAL ASSESSMENT	5 business days	We check the report for plausibility and reproducibility
STATUS UPDATE	10 business days	You will receive an initial assessment: Vulnerability confirmed / not confirmed / additional information required
REMEDIATION	Depending on severity	Critical/High: as soon as possible; Medium/Low: next scheduled release
PUBLICATION	After the fix is deployed	Security advisory naming the reporter (if desired)

4.2 Assessment

Vulnerabilities are rated according to the Common Vulnerability Scoring System (CVSS v3.1 or higher). Additionally, we take into account the EPSS score (Exploit Prediction Scoring System) and the actual deployment context of our products.

4.3 Coordinated Disclosure

We adhere to the principle of coordinated vulnerability disclosure:

- Vulnerability details are generally published only after a suitable mitigation has been provided, unless security interests or legal obligations require earlier disclosure.
- In cases of active exploitation or particular urgency, the regulatory authority is also informed and the deadline is shortened in consultation with the reporting party. The report is submitted to the relevant CSIRT and ENISA in accordance with the statutory requirements, as follows:
    - Early Warning – within 24 hours of becoming aware of the issue
    - Confirmation of Report/Detailed Report – within 72 hours of becoming aware of the issue
    - Final Report – no later than 14 days after a corrective measure is implemented (or within one month for serious incidents)

- If the resolution takes a very long time, we will coordinate with the reporting party regarding the publication of workarounds
- We reserve the right to inform customers confidentially in advance in the event of active exploitation, even if the fix is not yet available

4.4 Security Advisory

Once a fix has been provided, iris publishes a Security Advisory containing the following information:

- CVE ID (if assigned)
- Description of the vulnerability
- CVSS score
- Affected product versions
- Fixed product version
- Recommended Actions for Customers
- Acknowledgment of the Reporter (if desired)

Security advisories are published on the iris website.

5 What we expect from reporters

We ask everyone who reports vulnerabilities to adhere to the following principles:

- **Responsible Disclosure:** Do not publish any details about the vulnerability before a fix has been provided and the agreed-upon disclosure period has expired
- **No harm:** Do not exploit the vulnerability beyond what is necessary to demonstrate proof-of-concept
- **No data exfiltration:** Do not access data that does not belong to you, and do not copy, modify, or delete third-party data
- **No disruption of availability:** Do not take any actions that impair the availability of our products or services (e.g., denial-of-service)
- **No social engineering attacks:** Do not attempt to compromise iris employees, customers, or partners through social engineering
- **Compliance with Applicable Law:** Act in accordance with applicable law

6 What reporters can expect from us

- **No legal action:** iris will not take legal action against individuals who report vulnerabilities in good faith and in compliance with this policy—even if their research activities technically involve accessing iris systems
- **Confidentiality:** We will treat your identity and your report as confidential, unless you request otherwise
- **Recognition:** Upon request, we will credit you by name (or under a pseudonym) in the security advisory as the discoverer of the vulnerability
- **Transparency:** We will keep you updated on the status of our investigation and explain the reasoning behind our decisions
- **Timely Resolution:** We will address your report in accordance with the deadlines specified above

7 Security Updates and Patches

In accordance with the requirements of the EU Cyber Resilience Act, we provide security updates as follows:

- Security patches are provided free of charge to all affected customers
- Updates are delivered via secure distribution mechanisms
- Security updates are accompanied by a security advisory
- iris guarantees the resolution of vulnerabilities during the support period specified for each product. This period is in accordance with the requirements of the Cyber determined Resilience Act, taking into account the product's expected useful life.
- Customers will be notified of the end of the support period at least 6 months in advance, provided the product is still in use.