iris-GmbH infrared & intelligent sensors
Schnellerstr. 1–5 | 12439 Berlin
Germany

Richtlinie (PO)

Koordinierte Offenlegung von Sicherheitslücken in Produkten

Version:	1.0
Gültig ab:	01.09.2026
Vertraulichkeit:	öffentlich

Kontakt

Meldeportal: https://www.iris-sensing.com/de/support/
Security Advisories: https://www.iris-sensing.com/de/support/security-advisories/
E-Mail: informationsecurity@iris-sensing.com

Inhalt

1 Einleitung und Zweck 2
2 Geltungsbereich 2
3 Meldung einer Schwachstelle 3
4 Unser Umgang mit Ihrer Meldung 3
4.1 Prozessablauf und Fristen 3
4.2 Bewertung 3
4.3 Koordinierte Offenlegung 4
4.4 Security Advisory 4
5 Was wir von Meldenden erwarten 5
6 Was Meldende von uns erwarten dürfen 5
7 Sicherheits-Updates und Patches 6

1 Einleitung und Zweck

Die iris-GmbH infrared & intelligent sensors (im Folgenden nur „iris“) nimmt die Sicherheit ihrer Produkte und den Schutz ihrer Kunden sehr ernst. Wir sind davon überzeugt, dass die verantwortungsvolle Zusammenarbeit mit Sicherheitsforschern, Kunden, Partnern und der Öffentlichkeit ein wesentlicher Bestandteil der Produktsicherheit ist.

Dieses Dokument beschreibt, wie Schwachstellen in iris-Produkten an uns gemeldet werden können, was Meldende von uns erwarten dürfen und wie wir mit gemeldeten Schwachstellen umgehen. Sie unterstützt die Umsetzung der Anforderungen an den Umgang mit Schwachstellen gemäß Verordnung (EU) 2024/2847 (Cyber Resilience Act), insbesondere Annex I Part II.

Darüber hinaus ist die hier beschriebene Vorgehensweise in unser zertifiziertes Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 und in den sicheren Produktentwicklungsprozess nach IEC 62443-4-1 nahtlos integriert.

2 Geltungsbereich

Diese Leitlinie gilt für alle Produkte und Dienste der iris, insbesondere:

- Sensorhardware und eingebettete Firmware
- Begleitende Software, Konfigurationstools und Anwendungen
- Cloud-Dienste, die im Zusammenhang mit iris-Produkten betrieben werden
- Dokumentation und Konfigurationsanleitungen, soweit sicherheitsrelevant

Nicht im Geltungsbereich liegen Schwachstellen in eigenständigen Drittanbieter-Produkten, die nicht Bestandteil eines iris-Produkts oder -Dienstes sind.
Schwachstellen in Drittanbieter-Komponenten, die Bestandteil eines iris-Produkts sind, werden im Rahmen unseres Vulnerability-Handling-Prozesses berücksichtigt und erforderlichenfalls mit dem jeweiligen Hersteller koordiniert.

3 Meldung einer Schwachstelle

Schwachstellen können über den oben genannten Kontakt an uns gemeldet werden. Um eine effiziente Bearbeitung zu ermöglichen, bitten wir um folgende Angaben in der Meldung:

- **Betroffenes Produkt** und Produktversion
- **Version** der Firmware oder Software
- **Beschreibung der Schwachstelle** – Art der Schwachstelle, Zeitpunkt der Feststellung, Reproduzierbarkeit, evtl. mögliche Lösungsansätze
- **Quelle** – Ursprung der Erkennung (z. B. Vorfall, Penetrationstests, Schwachstellenscans)
- **Schweregrad** – Beschreibung der möglichen Auswirkungen bei Ausnutzung
- **Kontaktdaten** – Name (oder Pseudonym) und bevorzugte Kontaktmethode für Rückfragen

4 Unser Umgang mit Ihrer Meldung

4.1 Prozessablauf und Fristen

SCHRITT	FRIST	BESCHREIBUNG
EMPFANGSBESTÄTIGUNG	48 Stunden	Sie erhalten eine Bestätigung mit einer Referenznummer (Ticket-ID)
TRIAGE UND ERSTBEWERTUNG	5 Arbeitstage	Wir prüfen die Meldung auf Plausibilität und Reproduzierbarkeit
STATUS-UPDATE	10 Arbeitstage	Sie erhalten eine erste Einschätzung: Schwachstelle bestätigt / nicht bestätigt / weitere Informationen benötigt
BEHEBUNG	Gemäß Schweregrad	Kritisch/Hoch: schnellstmöglich; Mittel/Niedrig: nächstes geplantes Release
VERÖFFENTLICHUNG	Nach Fix-Bereitstellung	Security Advisory mit Nennung des Meldenden (sofern gewünscht)

4.2 Bewertung

Schwachstellen werden nach dem Common Vulnerability Scoring System (CVSS v3.1 oder höher) bewertet. Zusätzlich berücksichtigen wir den EPSS-Score (Exploit Prediction Scoring System) und den tatsächlichen Einsatzkontext unserer Produkte.

4.3 Koordinierte Offenlegung

Wir verfolgen den Grundsatz der koordinierten Offenlegung (Coordinated Vulnerability Disclosure):

- Schwachstellendetails werden grundsätzlich erst nach Bereitstellung einer geeigneten Abhilfemaßnahme veröffentlicht, sofern nicht Sicherheitsinteressen oder gesetzliche Verpflichtungen eine frühere Information erforderlich machen.
- Bei aktiver Ausnutzung oder besonderer Dringlichkeit wird zusätzlich die Aufsichtsbehörde informiert und die Frist in Abstimmung mit dem Meldenden verkürzt. Die Meldung erfolgt unter Beachtung der gesetzlichen Vorgaben an das zuständige CSIRT und die ENISA wie folgt:
    - Frühwarnung – innerhalb von 24 Stunden nach Kenntniserlangung
    - Meldebestätigung/Detailmeldung – innerhalb von 72 Stunden nach Kenntniserlangung
    - Abschlussbericht – spätestens 14 Tage nach Bereitstellung einer Abhilfemaßnahme (bzw. innerhalb eines Monats bei schwerwiegenden Vorfällen)

- Sollte die Behebung einen sehr langen Zeitraum in Anspruch nehmen, stimmen wir mit dem Meldenden die Veröffentlichung von Abhilfemaßnahmen (Workarounds) ab
- Wir behalten uns vor, bei aktiver Ausnutzung Kunden vorab vertraulich zu informieren, auch wenn der Fix noch nicht verfügbar ist

4.4 Security Advisory

Nach Bereitstellung eines Fixes veröffentlicht iris ein Security Advisory mit folgenden Informationen:

- CVE-ID (sofern vergeben)
- Beschreibung der Schwachstelle
- CVSS-Bewertung
- Betroffene Produktversionen
- Behobene Produktversion
- Empfohlene Maßnahmen für Kunden
- Anerkennung des Meldenden (sofern gewünscht)

Security Advisories werden auf der iris-Webseite veröffentlicht.

5 Was wir von Meldenden erwarten

Wir bitten alle Personen, die Schwachstellen melden, um die Einhaltung folgender Grundsätze:

- **Verantwortungsvolle Offenlegung:** Veröffentlichen Sie keine Details zur Schwachstelle, bevor ein Fix bereitgestellt wurde und die vereinbarte Offenlegungsfrist abgelaufen ist
- **Kein Schaden:** Nutzen Sie die Schwachstelle nicht über das für den Nachweis (Proof-of-Concept) erforderliche Maß hinaus aus
- **Keine Datenexfiltration:** Greifen Sie nicht auf Daten zu, die Ihnen nicht gehören, und kopieren, verändern oder löschen Sie keine fremden Daten
- **Keine Verfügbarkeitsstörung:** Führen Sie keine Aktionen durch, die die Verfügbarkeit unserer Produkte oder Dienste beeinträchtigen (z. B. Denial-of-Service)
- **Keine Social-Engineering-Angriffe:** Versuchen Sie nicht, iris-Mitarbeitende, Kunden oder Partner durch Social Engineering zu kompromittieren
- **Einhaltung geltenden Rechts:** Handeln Sie im Einklang mit geltendem Recht

6 Was Meldende von uns erwarten dürfen

- **Keine rechtlichen Schritte:** iris wird keine rechtlichen Schritte gegen Personen einleiten, die Schwachstellen in gutem Glauben und unter Einhaltung dieser Policy melden – auch wenn die Forschungsaktivitäten technisch einen Zugriff auf iris-Systeme beinhalten
- **Vertraulichkeit:** Wir behandeln Ihre Identität und Ihre Meldung vertraulich, sofern Sie nichts anderes wünschen
- **Anerkennung:** Auf Wunsch nennen wir Sie namentlich (oder unter Pseudonym) im Security Advisory als Entdecker der Schwachstelle
- **Transparenz:** Wir halten Sie über den Bearbeitungsstand auf dem Laufenden und begründen unsere Entscheidungen
- **Zeitnahe Bearbeitung:** Wir bearbeiten Ihre Meldung gemäß den oben genannten Fristen

7 Sicherheits-Updates und Patches

Gemäß den Anforderungen des EU Cyber Resilience Act stellen wir Sicherheitsupdates wie folgt bereit:

- Sicherheitspatches werden kostenlos an alle betroffenen Kunden bereitgestellt
- Updates werden über sichere Verteilmechanismen bereitgestellt
- Sicherheitsupdates werden von einem Security Advisory begleitet
- iris gewährleistet die Behandlung von Schwachstellen während des für das jeweilige Produkt festgelegten Supportzeitraums. Dieser wird gemäß den Anforderungen des Cyber Resilience Act unter Berücksichtigung der erwarteten Nutzungsdauer des Produkts bestimmt.
- Das Ende des Unterstützungszeitraums wird Kunden mindestens 6 Monate im Voraus angekündigt, sofern das Produkt weiterhin im Einsatz ist.