Allied Vision
www.alliedvision.com
quality@alliedvision.com

Konzept für die koordinierte Offenlegung von Schwachstellen

1. Allgemeines

Zweck:
In Umsetzung des EU Cyber Resilience Act (Verordnung 2024/2847), beschreibt dieses Konzept, wie Allied Vision Sicherheitslücken in Produkten und zugehörigen Services koordiniert annimmt, bewertet, behebt und kommuniziert, um Risiken für Nutzer und Dritte zu minimieren.

Geltungsbereich:
Gilt für alle von Allied Vision entwickelten und vertriebenen Produkte/Software/Firmware, einschließlich Abhängigkeiten, sofern Allied Vision Einfluss auf Behebung oder Mitigation hat. Ausgenommen: Schwachstellen in Third-Party-Produkten außerhalb unseres Einflusses (werden weitergeleitet/eskaliert).

Grundprinzipien:

- Koordinierte Informationen statt „Full Disclosure“ ohne Vorwarnung
- Faire Behandlung von Meldenden (Good-Faith)
- Nachvollziehbare Dokumentation und Fristen
- Vertrauliche Behandlung sicherheitsrelevanter Informationen bis zur Behebung

Sitz des Unternehmens und zuständiges CSIRT

- Schwerpunkt der CRA-relevanten Aktivitäten ist Deutschland, deshalb gilt Deutschland nach Artikel 14 CRA als Unternehmenssitz und das zuständige CSIRT ist das CERT-Bund beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

Begriffe

- Schwachstelle (Vulnerability): Schwäche in einem Produkt mit digitalen Elementen, die zur unbefugten Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit ausgenutzt werden kann.
- Sicherheitsvorfall (Incident): Ereignis, das die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität von Daten oder Diensten beeinträchtigt.
- Aktiv ausgenutzte Schwachstelle: Nachweisliche Ausnutzung einer Schwachstelle ohne Zustimmung des Systemeigentümers, z. B. belegt durch Threat-Intelligence, die European Vulnerability Database oder validierte Kundenmeldung.
- Koordinierte Offenlegung (Coordinated Vulnerability Disclosure): Abgestimmter Veröffentlichungszeitpunkt zwischen Allied Vision und Meldendem/Behörden gemäß u.g. Abschnitt 8.
- Support-Zeitraum: Der von Allied Vision je Produkt erklärte Zeitraum, in dem Sicherheitsupdates bereitgestellt werden (der Produktdokumentation zu entnehmen).

- Single Point of Contact (SPOC): diejenige Stelle, an der alle Informationen zusammenlaufen und von der alle Kommunikation ausgeht (Kommunikationsportal und das dahinterliegende Personal).
- Product Security Incident Response Team (PSIRT): ein Team von Fachleuten, das auf globaler bzw. lokaler Ebene für die Ausführung des hier beschriebenen Prozesses verantwortlich ist.

---

2. Rollen und Verantwortlichkeiten

Quality and Compliance Management:

- Personeller Teil des SPOC für eingehende und ausgehende Meldungen (global), Kommunikation mit den Meldenden.
- Koordination der PSIRT (lokal)
- Prüfung rechtlicher Aspekte
- Durchführung der Behördenmeldung an ENISA/CERT-Bund

Das Quality Management Team hat dafür Vertretungsregelungen festgelegt.

Product Security Incident Response Team (PSIRT):

- Kategorisierung, Validierung, Priorisierung, Koordination mit Produktteams
- Kommunikation mit Meldenden und ggf. Behörden/CSIRTs
- Veröffentlichung von Advisories

PSIRT – Mitglieder sind auf globaler und lokaler Ebene benannt und werden von QM koordiniert.

Engineering Team (als Teil des PSIRT):

- Technische Analyse, Fix/Mitigation, Tests, Freigabeplanung
- Pflege von SBOM/Komponenteninfos (soweit vorhanden)

Applications Engineering (als Teil des PSIRT):

- Einbindung bei Kundenkommunikation/Workarounds/Mitigation

Produkt- und Materialbuchung (als Teil des PSIRT):

- Arbeitet bei Bedarf die notwendigen Informationen zur Nachverfolgbarkeit von Verkäufen, Käufen, sonstigen Materialbewegungen, Lagerbeständen, offenen Bestellungen zu.

---

3. Meldekanäle (Vulnerability Intake)

Meldungen können eingereicht werden über:

- **Durch Kunden und andere Externe:** SPOC/ Web-Formular: https://www.alliedvision.com/de/company/legal-and-compliance/cybersecurity
- Durch Interne: E-Mail: quality@alliedvision.com (nachgelagerter Teil des SPOC)

Erforderliche Angaben:

- Betroffenes Produkt (Artikelnummer, Seriennummer(n)
- Beschreibung der Schwachstelle und Auswirkung
- Reproduktionsschritte / Proof of Concept (wenn möglich)
- Beobachtete/erwartete Sicherheitswirkung
- Kontakt für Rückfragen
- **Optional:** Logs, Screenshots, Exploitability Details

---

4. Safe-Harbor / Good-Faith Zusicherung

Allied Vision verpflichtet sich, Meldende wegen **Sicherheitsforschung, die in gutem Glauben durchgeführt wurde,** nicht rechtlich zu verfolgen, sofern sie:

- nur minimale, notwendige Tests durchführen,
- keine Daten exfiltrieren, verändern oder dauerhaft beeinträchtigen,
- keine Social Engineering und/ oder Phishing gegen Mitarbeitende einsetzen,
- die Rechte Dritter durch ihre Tests nicht verletzen,
- die Schwachstelle nicht öffentlich machen, bevor ein Koordinationszeitplan vereinbart ist (siehe Abschnitt 8),
- geltende Gesetze beachten.

Wenn unbeabsichtigt personenbezogene Daten eingesehen werden: **sofort stoppen**, Daten nicht speichern/weitergeben und Allied Vision über den oben genannten Meldekanal informieren.

Ein Fehlverhalten des Meldenden hebt für Allied Vision die Behebungspflicht bei einer real existierenden Schwachstelle nicht auf.

---

5. Prozessübersicht (End-to-End)

Prozesskette: Eingang → Bestätigung → Kategorisierung → Validierung → Priorisierung → Sofortmaßnahmen → Maßnahmenplan und weitergehende Grundursachenanalyse → Behebung/Mitigation → Verifizierung → Release/Deployment/Advisory Disclosure → Vorbeugemaßnahmen und Nachbearbeitung.

5.1 Eingang & Bestätigung

- Der Prozess kann gestartet werden durch:
    - Kundenmeldung (siehe 3.)
    - interne Meldung (Penetration Tests, Erkenntnisse aus öffentlichen Cybersecurity-Datenbanken wie ENISA.
- QM vergibt eine **Ticket-ID** und ermittelt einen Ansprechpartner.
- QM bestätigt den Eingang an die Meldenden **schnellstmöglich** mit Ticket ID und Ansprechpartner

5.2 Kategorisierung

- Ersteinschätzung durch QM (ggf. mit Support durch das Engineering Team), ob der Report plausibel ist und in den Scope fällt.
  Mögliche Ergebnisse: **valid/ not valid (not reproducible / out of scope / duplicate)**.
- Bei Ergebnis „not valid“ wird der Meldende informiert und ggf. um weitere Informationen für eine Neubewertung gebeten. Der Vorgang mit Begründung geschlossen, wenn die Kommunikation mit dem Meldenden abgeschlossen ist.

5.3 Validierung und Priorisierung (nach Schweregrad)

- Bei Ergebnis „valid“ erfolgt die weitere Validierung durch das Engineering Team.
    - Die Kriterien für „aktive Ausnutzung einer Schwachstelle“ bzw. einen „schwerwiegenden Sicherheitsvorfall“ richten sich nach den Definitionen des CRA-Artikel 3, Punkte 42 und 44.

Validierte Meldungen werden priorisiert:

- **Critical** (u.a.: ausgenutzte Schwachstelle, Remote Code Execution, Authentification Bypass, massenhaft ausnutzbar)
- **High** (potenzielle Ausnutzung hat hohen Impact)
- **Medium** (potenzielle Ausnutzung hat geringen Impact)
- **Low** (Schwachstelle nicht ausnutzbar). Bei diesen Fällen wird der Vorgang geschlossen und ggf. ohne Fristsetzung durch Engineering im Entwicklungsprozess weiterbearbeitet.

5.4 Sofortmaßnahmen

- Sobald die aktive Ausnutzung einer Schwachstelle bzw. ein schwerwiegender Sicherheitsvorfall validiert ist, meldet QM dies spätestens 24 Stunden nach Validierung an CERT-BUND und ENISA. Weitere Meldepflichten an CERT-Bund und ENISA mit Fristen: siehe Abschnitt 6.
- Meldende werden über das Ergebnis informiert (mit Begründung).
- Bei „Critical“ und „High“ wird die weitere Information wesentlicher Stakeholder (CERT-BUND, ENISA, Meldende, Kunden) geplant und nach dem dokumentierten Plan ausgeführt.

5.5 Maßnahmenplan und weitergehende Grundursachenanalyse

- Ein Maßnahmenplan wird erstellt, der die unten genannten Schritte sowie die Information von Behörden, Meldenden und Kunden umfasst.
- Ist die Grundursache hinter dem identifizierten Fehler noch unklar, wird diese nun ermittelt.

5.6 Behebung & Mitigation

- Das Engineering Team erstellt einen Fix/Workaround.
- Falls ein sofortiger Fix nicht möglich ist: **Mitigation** (Konfig, WAF Rule, Feature Flag, Rate limiting etc.).
- Sicherheitsrelevante Änderungen erhalten einen Security Review und Regression-Tests.

5.7 Verifizierung

- Der Fix wird gegen Proof of Concept (PoC) geprüft; wenn möglich wird der Meldende um eine Wiederholungsprüfung gebeten.
- Betroffene Versionen sowie Bedarf nach Downgrading werden ermittelt.

5.8 Release/Deployment/Advisory Disclosure

- Ein Patch wird über die Webseite veröffentlicht (siehe 3. SPOC).
- Release Notes und Upgrade-Anleitung werden an Meldenden geschickt und allgemein über die Webseite (siehe 3. SPOC) veröffentlicht.
- Ggf. werden Advisories auf der Webseite veröffentlicht (SPOC)

5.9 Vorbeugemaßnahmen und Nachbearbeitung

- Auf Basis der Grundursachenanalyse und weiterer Erkenntnisse (Lessons Learned) werden ggf. Secure- Software Development Life Cycle-Verbesserung oder andere Vorbeugemaßnahmen in Verantwortung von Engineering ausgeführt.
- Threat Models, Secure Coding Guidelines, Testfälle werden aktualisiert.

---

6. Zeitvorgaben

Melde- und Berichtspflichten gegenüber CERT-Bund und ENISA

Sofern bei Produkten mit digitalen Elementen im Anwendungsbereich des EU Cyber Resilience Act (CRA) die aktive Ausnutzung einer Schwachstelle oder ein schwerwiegender Sicherheitsvorfall validiert wurden, bestehen nach Artikel 14 CRA verbindliche Meldefristen gegenüber CERT-Bund bzw. ENISA, die von Allied Vision eingehalten werden:

- Frühwarnung (Early Warning): innerhalb von 24 Stunden.
- Meldung (Notification): innerhalb von 72 Stunden mit einer ersten Bewertung, Schweregrad und ggf. Kompromittierungsindikatoren.
- Abschlussbericht (Final Report):
    - **Critical**: Abschlussbericht spätestens nach 14 Tagen.

    - **Medium-High**: Abschlussbericht spätestens 14 Tage, nachdem eine Abhilfe- oder Mitigationsmaßnahme verfügbar ist, jedoch spätestens innerhalb eines Monats.

- Verantwortlich für die Behördenmeldung: Quality and Compliance Management (SPOC) ggf. in Abstimmung mit den Rechtsberatern des Unternehmens.
- Unabhängig davon bleiben Meldepflichten nach DSGVO Art. 33/34 (72 Stunden) bestehen, sofern personenbezogene Daten betroffen sind (siehe Abschnitt 4).

Darüber hinaus gelten die folgenden **Zielwerte** (die Zeiten richten sich nach der Kritikalität, die aus der Meldung des Kunden ableitbar ist, bei dringendem Verdacht auf aktive Ausnutzung mit schwerwiegenden Folgen werden die Fristen verkürzt):

- **Eingangsbestätigung:** ≤ 2 Arbeitstage
- **Kategorisierung & Validierung:**
    - Wenn vermutete Kritikalität „high“ oder „critical“: ≤ 5 Arbeitstage
    - Wenn vermutete Kritikalität „low“ oder „medium“: ≤ 15 Arbeitstage
- **Ziel zur Beendigung der Abstellmaßnahmen**:
    - Critical: ≤ 15–30 Tage (oder ASAP bei Exploitation)
    - High: ≤ 60 Tage
    - Medium: ≤ 90 Tage
    - Low: nach Release-Zyklus, i. d. R. ≤ 180 Tage

Wenn ein Fix länger dauert: PSIRT informiert den Meldenden mit Begründung und neuem Zeitplan.

---

7. Kommunikation & Koordination

Mit Meldenden:

- Regelmäßige Updates (alle 14 Tage bei High/Critical, sonst monatlich).
- Klare Absprachen über Veröffentlichungszeitpunkt.

Mit Kunden/Öffentlichkeit:

- Veröffentlichung von Schwachstellen auf der Webseite (siehe 3. SPOC).
- Bei erheblichen Risiken wird ein **Security Advisor** veröffentlicht (siehe 3. SPOC).
- Advisory enthält: Beschreibung, betroffene Versionen, Impact, Score dem nach Common Vulnerability Scoring System (CVSS), Mitigations, Fix-Versionen.

Mit externen Stellen:

- Ggf. Meldung an CERT-BUND und ENISA nach den Vorgaben der Verordnung (siehe 5.4).

Mit Internen Abteilungen:

- Kommunikation und Dokumentation innerhalb der PSIRT via Jira.
- Kommunikation mit der Geschäftsleitung durch QM bei schwerwiegenden Fällen.
- Einbinden der externen Rechtsberater durch QM oder Geschäftsleitung bei Bedarf.

---

8. Disclosure-Regeln (Koordinierte Veröffentlichung)

Grundsatz: Allied Vision und Meldender streben eine koordinierte Veröffentlichung an, sobald ein Fix oder wirksame Mitigation verfügbar ist.

Standard:

- Veröffentlichung spätestens **90 Tage** nach Validierung, **oder** früher bei verfügbarem Patch.
- Verlängerung möglich, wenn (a) Fix komplex ist, (b) Nutzer-Ökosystem längere Rollout-Zeiten braucht, (c) keine Hinweise auf aktive Ausnutzung vorliegen.
- Bei **active exploitation** kann Allied Vision früher warnen (auch ohne finalen Fix), um Nutzer zu schützen.

Vorzeitige Veröffentlichung durch Meldende:
Wir bitten Meldende, bei geplanter Veröffentlichung vor Ablauf des Zeitplans Rücksprache mit uns zu halten; bei unkoordinierter Veröffentlichung priorisieren wir Schutzmaßnahmen und Kommunikation.

Unbenommen dessen gelten die oben genannten Meldepflichten.

---

9. Umgang mit sensiblen Informationen

- Details, Proof of Concept und technische Exploit-Informationen werden nach dem Prinzip „need-to-know“ behandelt.
- Zugriff nur für die an der Analyse und Lösung Beteiligten (v.a. PSIRT)
- Speicherung in gesicherten Systemen (Ticketing mit Zugriffskontrolle, Verschlüsselung).
- Sensible Daten werden, nach dem bei Allied Vision geltenden System klassifiziert.
- Sensible Daten werden gelöscht, sobald sie nicht mehr benötigt werden und sofern gesetzliche Vorgaben dem nicht entgegenstehen.

---

10. Schwachstellenklassifizierung & Identifikatoren

- Pro Meldung wird eine interne ID vergeben und für die weitere Bearbeitung des Vorgangs inklusive jeglicher Kommunikation und Dokumentation genutzt.
- Falls angemessen, wird ein „Common Vulnerabilities and Exposures“ (CVE) beantragt/ koordiniert.
- Advisories referenzieren Fix-Versionen und ggf. CVE.

11. Abhängigkeiten / Third-Party Komponenten

Wenn Schwachstellen in Drittkomponenten liegen:

- PSIRT koordiniert die Bearbeitung mit dem Lieferanten/ Hersteller der Komponente.
- Die Kundenkommunikation enthält klare Hinweise zu betroffenen Versionen und Workarounds.
- Wenn der Lieferant wiederholt nicht reagiert, ergreift PSIRT eigene Mitigationsmaßnahmen.
    - Der Lieferant wird neu bewertet, ihm werden das Ergebnis der Bewertung und die Konsequenzen daraus mitgeteilt (Bei chinesischen Lieferanten zu beachten: ein Ausphasen aufgrund von EU-Gesetzen ist dort mit Sanktionen belegt).
    - Bei gesichertem/validiertem Risiko: analog zu Abschnitt 5.5ff vorgehen.
    - Bei vermutetem Risiko: werden weitere Bewertungen durchgeführt, mit dem Ziel, das Risiko zu klassifizieren und zu validieren. Danach analog zu Abschnitt 5.5 ff vorgehen.

12. Policy-Verstöße und Missbrauch

Allied Vision kann Meldungen ablehnen, wenn sie enthalten:

- Erpressung („pay or disclose“); hier erfolgt Meldung an die zuständigen Strafverfolgungsbehörden.
- absichtliche Datenentnahme oder Serviceunterbrechung,
- massenhafte automatisierte Scans gegen produktive Systeme ohne Zustimmung,
- Social Engineering.

Ein Fehlverhalten des Meldenden hebt für Allied Vision die Behebungspflicht bei einer real existierenden Schwachstelle nicht auf.

13. Versionierung, Review und Training

- Eigner dieses Dokuments: PSIRT Lead (QM).
- Review: mindestens jährlich oder nach Major Incident oder nach Änderung der Rechtslage (Cyber Resilience Act).
- Schulung: für PSIRT-Mitglieder zu Eingang, Ablauf, Eskalation und Geheimhaltung.
- Dokumentation: im Dokumentenmanagementsystem des Unternehmens (Q.Wiki).

Anhang A: Vorlage Eingangsbestätigung (E-Mail)

Betreff: [Ticket-ID] Vulnerability Report – Eingang bestätigt

Danke für Ihre Meldung. Wir haben den Report unter der ID **[Ticket-ID]** registriert.
Wir melden uns spätestens bis **[Datum]** mit der ersten Einschätzung/Validierung.
Sie erreichen uns unter quality@alliedvision.com.

Für Kommunikation sensibler Daten nutzen Sie bitte S/Mime zur Verschlüsselung von E-Mails oder fordern bei uns einen gesicherten Zugang an.

Anhang B: Security Advisory Template (für die Webseite)

Titel: [Produkt] – [CVE-XXXX-YYYY] – [Kurzimpact]
Datum: [YYYY-MM-DD]
Schweregrad: [Critical/High/Medium/Low] (CVSS v4.0: [Score], Vector: [..])
Betroffene Produkte: [Modelle/HW-Rev], [Firmware-Versionen],
Zusammenfassung: [2–4 Sätze]
Technische Details: [so viel wie nötig, so wenig wie möglich]
Mitigations/Workarounds: [Schritte]
Fix: [Version/OTA Rollout Datum/Manual Update]
Timeline: [Reported/Analyzed/Fixed/Disclosed] (optional)

Anhang C: Statusupdate-Vorlage (E-Mail)

Betreff: [Ticket-ID] Vulnerability Report – Status-Update

Wir informieren Sie zum Stand Ihrer Meldung [Ticket-ID]. Aktueller Status: [Status]. Nächstes geplantes Update: [Datum]. Bei Rückfragen erreichen Sie uns unter quality@alliedvision.com.

Anhang D: Ablehnungs-Vorlage (E-Mail)

Betreff: [Ticket-ID] Vulnerability Report – Rückmeldung

Vielen Dank für Ihre Meldung [Ticket-ID]. Nach Prüfung stufen wir den Report als [Not reproducible / Out of scope / Duplicate] ein. Begründung: [Begründung]. Bei neuen Erkenntnissen können Sie den Report gerne erneut einreichen.