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

Coordinated vulnerability disclosure approach

1. General

Purpose: In implementation of the EU Cyber Resilience Act (Regulation 2024/2847), this concept describes how Allied Vision administers, assesses, remediates, and communicates security vulnerabilities in products and related services in a coordinated manner to minimize risks to users and third parties.

Scope:
Applies to all products/software/firmware developed and distributed by Allied Vision, including dependencies where Allied Vision has control over remediation or mitigation. Excluded: Vulnerabilities in third-party products beyond our control (will be forwarded/escalated).

Basic principles:

- Coordinated information instead of "full disclosure" without warning
- Fair treatment of notifiers (GoodFaith)
- Comprehensible documentation and deadlines
- Confidentiality of security-related information until remediation

Registered office of the company and responsible CSIRT

- The focus of CRA-relevant activities is Germany, which is why Germany is considered the company's headquarters according to Article 14 CRA and the responsible CSIRT is the CERT-Bund at the Federal Office for Information Security (BSI).

Terms

- Vulnerability: A weakness in a product with digital elements that can be exploited to compromise confidentiality, integrity, or availability without authorization.
- Security Incident: An event that affects availability, confidentiality, integrity, or authenticity of data or services.
- Actively exploited vulnerability: Proven exploitation of a vulnerability without the consent of the system owner, e.g. proven by threat intelligence, the European Vulnerability Database or validated customer notification.
- Coordinated Vulnerability Disclosure: Coordinated publication timing between Allied Vision and the notifier/authorities in accordance with Section 8 below.
- Support Period: The period declared by Allied Vision per product during which security updates are provided (see product documentation).
- Single Point of Contact (SPOC): the point where all information converges and from which all communication originates (communication portal and the personnel behind it).
- Product Security Incident Response Team (PSIRT): a team of professionals responsible for executing the process described herein at a global or local level.

2. Roles and responsibilities

Quality and Compliance Management:

- Personnel part of the SPOC for incoming and outgoing reports (global), communication with the notifiers.
- Coordination of the PSIRT (local)
- Examination of legal aspects
- Implementation of the official notification to ENISA/CERT-Bund

The Quality Management Team has defined substitution regulations for this purpose.

Product Security Incident Response Team (PSIRT):

- Categorization, validation, prioritization, coordination with product teams
- Communication with notifiers and, if applicable, authorities/CSIRTs
- Publication of advisories

PSIRT members are appointed at the global and local level and are coordinated by QM.

Engineering Team (as part of the PSIRT):

- Technical analysis, fix/mitigation, testing, release planning
- Maintenance of SBOM/component information (if available)

Applications Engineering (as part of the PSIRT):

- Involvement in customer communication/workarounds/mitigation

Product and material booking (as part of the PSIRT):

- If necessary, provides the necessary information for the traceability of sales, purchases, other material movements, inventories, and open orders.

3. Vulnerability Intake

Reports can be submitted:

- **By customers and other external parties:** SPOC/ Web form: https://www.alliedvision.com/de/company/legal-and-compliance/cybersecurity
- By Internal: Email: quality@alliedvision.com (downstream part of the SPOC)

Required information:

- Affected product (article number, serial number(s))
- Description of the vulnerability and impact
- Reproduction steps / proof of concept (if possible)
- Observed/expected safety effect
- Contact for enquiries
- **Optional:** Logs, Screenshots, Exploitability Details

---

4. Safe-Harbor/Good-Faith Assurance

Allied Vision commits not to prosecute notifiers for **security research conducted in good faith** if they:

- carry out only minimal, necessary tests,
- not exfiltrate, alter or permanently impair data,
- do not use social engineering and/or phishing against employees,
- do not violate the rights of third parties through their tests,
- do not make the vulnerability public before a coordination timeline has been agreed (see section 8);
- comply with applicable laws.

If personal data is unintentionally viewed: **stop immediately**, do not store/share data and inform Allied Vision via the above reporting channel.

Misconduct by the notifier does not remove the obligation for Allied Vision to remedy a real existing vulnerability.

---

5. Process overview (end-to-end)

Process chain: Receipt → confirmation → categorization → validation → prioritization → immediate measures → action plan and further root cause analysis → remediation/mitigation → verification → release/deployment/advisory disclosure → preventive measures and follow-up.

5.1 Receipt & Acknowledgment

- The process can be started by:
    - Customer report (see 3.)
    - internal reporting (penetration tests, findings from public cybersecurity databases such as ENISA.
- QM assigns a **ticket ID** and determines a contact person.
- QM will confirm receipt to the notifiers **as soon as possible** with ticket ID and contact person

5.2 Categorization

- Initial assessment by QM (if necessary, with support from the engineering team) as to whether the report is plausible and falls within the scope.
  Possible results: **valid/ not valid (not reproducible / out of scope / duplicate).**
- If the result is "not valid", the notifier is informed and, if necessary, asked for further information for a reassessment. The process is closed with justification when communication with the notifier is completed.

5.3 Validation and prioritization (by severity)

- If the result is "valid", further validation will be carried out by the engineering team.
    - The criteria for "active exploitation of a vulnerability" and a "serious security incident" are based on the definitions of CRA Article 3, points 42 and 44.

Validated messages are prioritized:

- **Critical** (e.g.: exploited vulnerability, remote code execution, authentication bypass, mass exploitation)
- **High** (potential exploitation has high impact)
- **Medium** (potential exploitation has low impact)
- **Low** (vulnerability not exploitable). In these cases, the process is closed and, if necessary, further processed by engineering in the development process without setting a deadline.

5.4 Immediate actions

- As soon as the active exploitation of a vulnerability or a serious security incident is validated, QM reports it to CERT-BUND and ENISA no later than 24 hours after validation. Further reporting obligations to CERT-Bund and ENISA with deadlines: see section 6.
- Notifiers will be informed of the result (with justification).
- In the case of "Critical" and "High", further information of key stakeholders (CERT-BUND, ENISA, notifiers, customers) is planned and carried out according to the documented plan.

5.5 Action plan and further root cause analysis

- An action plan will be drawn up that includes the steps listed below as well as informing authorities, notifiers and customers.
- If the root cause behind the identified fault is still unclear, it will now be determined.

5.6 Remediation & Mitigation

- The engineering team creates a fix/workaround.
- If an immediate fix is not possible: **Mitigation** (config, WAF rule, feature flag, rate limiting etc.).
- Security-relevant changes receive a security review and regression tests.

5.7 Verification

- The fix will be checked against Proof of Concept (PoC); if possible, the notifier will be asked to recheck.
- Affected versions as well as the need for downgrading are determined.

5.8 Release/Deployment/Advisory Disclosure

- A patch will be released via the website (see 3rd SPOC).
- Release notes and upgrade instructions will be sent to notifiers and generally published via the website (see 3rd SPOC).
- If applicable, advisories will be published on the website (SPOC).

5.9 Preventive actions and follow-up

- Based on the root cause analysis and further findings (lessons learned), secure software development life cycle improvement or other preventive measures are carried out under the responsibility of Engineering.
- Threat models, secure coding guidelines, test cases are updated.

---

6. Time constraints

Notification and Reporting Requirements to CERT-Bund and ENISA

If the active exploitation of a vulnerability or a serious security incident has been validated for products with digital elements within the scope of the EU Cyber Resilience Act (CRA), there are binding reporting deadlines to CERT-Bund or ENISA in accordance with Article 14 CRA, which are complied with by Allied Vision:

- Early Warning: within 24 hours.
- Notification: within 72 hours with an initial assessment, severity and, if applicable, indicators of compromise.
- Final Report:
    - **Critical**: Final report after 14 days at the latest.

    - **Medium-High**: Final report no later than 14 days after a remedial or mitigation action becomes available, but no later than one month.

- Responsible for reporting to the authorities: Quality and Compliance Management (SPOC), if necessary, in coordination with the company's legal advisors.
- Irrespective of this, reporting obligations under GDPR Art. 33/34 (72 hours) remain in place if personal data is affected (see section 4).

In addition, the following **target values** apply (the timeframes depend on the level of criticality, which can be determined from the customer's report; if there is strong suspicion of active exploitation with serious consequences, the deadlines are shortened):

- **Confirmation of receipt:** ≤ 2 working days
- **Categorization & Validation:**
    - If suspected criticality "high" or "critical": ≤ 5 working days
    - If suspected criticality low or medium: ≤ 15 working days
- **Goal to end the remedial measures**:
    - Critical: ≤ 15-30 days (or ASAP in case of exploitation)
    - High: ≤ 60 days
    - Medium: ≤ 90 days
    - Low: after release cycle, usually ≤ 180 days

If a fix takes longer than expected: PSIRT notifies the notifier, providing an explanation and a new timeline.

---

7. Communication & Coordination

With registrants:

- Regular updates (every 14 days for High/Critical, otherwise monthly).
- Clear agreements on release dates.

With customers/public:

- Disclosure of vulnerabilities on the website (see 3rd SPOC).
- In the event of significant risks, a **security advisor** is published (see 3rd SPOC).
- Advisory includes: description, affected versions, impact, score according to Common Vulnerability Scoring System (CVSS), mitigations, fix versions.

With external bodies:

- If necessary, notification to CERT-BUND and ENISA in accordance with the requirements of the regulation (see 5.4).

With internal departments:

- Communication and documentation within PSIRT via Jira.
- Communication with the management through QM in serious cases.
- Involvement of external legal advisors by QM or management if necessary.

---

8. Disclosure Rules (Coordinated Publication)

Principle: Allied Vision and the notifier aim for a coordinated release as soon as a fix or effective mitigation is available.

Standard:

- Release no later than **90 days** after validation, **or** sooner if patch is available.
- Extension possible if (a) fix is complex, (b) user ecosystem needs longer rollout times, (c) there is no evidence of active exploitation.
- With **active exploitation**, Allied Vision can warn earlier (even without a final fix) to protect users.

Early publication by notifiers:
We ask notifiers to consult with us if they want to publish before the end of the schedule; in the event of uncoordinated disclosure, we prioritize protective measures and communication.

Notwithstanding this, the above-mentioned reporting obligations apply.

---

9. Handling of sensitive information

- Details, proof of concept, and technical exploit information are handled on a need-to-know basis.
- Access restricted to those involved in analysis and resolution (primarily PSIRT).
- Storage in secure systems (ticketing with access control, encryption).
- Sensitive data is classified according to the system in force at Allied Vision.
- Sensitive data is deleted as soon as it is no longer needed and provided that no legal requirements prevent this.

---

10. Vulnerability Classification & Identifiers

- An internal ID is assigned to each report and used for further processing, including any communication and documentation.
- If appropriate, a "Common Vulnerabilities and Exposures" (CVE) is requested/coordinated.
- Advisories reference fix versions and, if applicable, CVE.

---

11. Dependencies / Third-Party Components

If vulnerabilities lie in third-party components:

- PSIRT coordinates the machining with the supplier/manufacturer of the component.
- Customer communication contains clear information on affected versions and workarounds.
- If the supplier repeatedly fails to respond, PSIRT takes its own mitigation measures.
    - The supplier is re-evaluated, he is informed of the result of the evaluation and the consequences of it (note in the case of Chinese suppliers: phase-out due to EU laws is subject to sanctions there).
    - If the risk is secured/validated: proceed analogous to sections 5.5ff.
    - If the risk is suspected: further assessments are carried out with the aim of classifying and validating the risk. Then proceed analogous to sections 5.5ff.

---

12. Policy Violations and Abuse

Allied Vision may reject messages if they contain:

- extortion ("pay or disclose"); in this case, a report is made to the appropriate law enforcement authorities.
- deliberate data extraction or service interruption,
- mass automated scans against productive systems without consent,
- Social Engineering.

Misconduct on the part of the reporter does not relieve Allied Vision of its obligation to address a genuine vulnerability.

---

13. Versioning, Review, and Training

- Owner of this document: PSIRT Lead (QM).
- Review: at least annually or after major incident or after a change in the legal situation (Cyber Resilience Act).
- Training: for PSIRT members on receipt, procedures, escalation, and confidentiality.
- Documentation: in the company's document management system (Q.Wiki).

Appendix A: Template acknowledgement of receipt (e-mail)

Subject: [Ticket-ID] Vulnerability Report – Receipt acknowledged

Thank you for your report. We have registered the notification under the ID **[Ticket ID].** We will get back to you by **[date]** at the latest with the first assessment/validation.
You can reach us at quality@alliedvision.com.

For communication of sensitive data, please use S/MIME to encrypt e-mails or request secure access from us.

Appendix B: Security Advisory Template (for the website)

Title: [Product] – [CVE-XXXX-YYYY] – [Short Impact]
Date: [YYYY-MM-DD]
Severity: [Critical/High/Medium/Low] (CVSS v4.0: [Score], Vector: [..])
Affected Products: [Models/HWRev], [Firmware Versions],
Summary: [2–4 sentences]
Technical Details: [as much as needed, as little as possible]
Mitigations/Workarounds: [Steps]
Fix: [Version/OTA Rollout Date/Manual Update]
Timeline: [Reported/Analyzed/Fixed/Disclosed] (optional)

Appendix C: Status Update Template (Email)

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

We are providing an update on the status of your report [Ticket ID]. Current status: [Status]. Next scheduled update: [Date]. If you have any questions, you can reach us at quality@alliedvision.com.

Appendix D: Rejection Template (Email)

Subject: [Ticket ID] Vulnerability Notification – Feedback

Thank you for your notification [ticket ID]. After reviewing it, we have classified the notification as [Not reproducible / Out of scope / Duplicate]. Reason: [Reason]. If you have any new information, please feel free to resubmit the notification.