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

Linee guida per la segnalazione coordinata delle vulnerabilità

1. Informazioni generali

Scopo:
In attuazione del Cyber Resilience Act dell'UE (Regolamento 2024/2847), le presenti linee guida descrivono le modalità con cui Allied Vision riceve, valuta, risolve e comunica in modo coordinato le vulnerabilità presenti nei prodotti e nei servizi correlati, al fine di ridurre al minimo i rischi per gli utenti e i terzi.

Ambito di applicazione:

Si applica a tutti i prodotti/software/firmware sviluppati e distribuiti da Allied Vision, comprese le dipendenze, nella misura in cui Allied Vision abbia influenza sulla risoluzione o sulla mitigazione.

Esclusioni: vulnerabilità nei prodotti di terze parti al di fuori del nostro controllo (vengono inoltrate/scalate).

Principi fondamentali:

- Informazioni coordinate anziché «full disclosure» senza preavviso
- Trattamento equo dei segnalanti (buona fede)
- Documentazione trasparente e scadenze chiare
- Trattamento riservato delle informazioni rilevanti per la sicurezza fino alla risoluzione del problema

Sede dell'azienda e CSIRT competente

- Il fulcro delle attività rilevanti ai sensi del CRA è la Germania; pertanto, ai sensi dell'articolo 14 del CRA, la Germania è considerata la sede dell'azienda e il CSIRT competente è il CERT-Bund presso l'Ufficio federale per la sicurezza informatica (BSI).

Termini

- Vulnerabilità (Vulnerability): punto debole in un prodotto con elementi digitali che può essere sfruttato per compromettere in modo non autorizzato la riservatezza, l'integrità o la disponibilità.
- Incidente di sicurezza (Incident): evento che compromette la disponibilità, la riservatezza, l'integrità o l'autenticità di dati o servizi.
- Vulnerabilità attivamente sfruttata: sfruttamento comprovato di una vulnerabilità senza il consenso del proprietario del sistema, ad esempio documentato da informazioni di intelligence sulle minacce, dall'European Vulnerability Database o da una segnalazione convalidata da parte di un cliente.
- Divulgazione coordinata (Coordinated Vulnerability Disclosure): momento di pubblicazione concordato tra Allied Vision e il segnalante/le autorità ai sensi della sezione 8 riportata di seguito.

- Periodo di supporto: il periodo dichiarato da Allied Vision per ciascun prodotto durante il quale vengono forniti aggiornamenti di sicurezza (da consultare nella documentazione del prodotto).
- Single Point of Contact (SPOC): il punto di riferimento in cui confluiscono tutte le informazioni e da cui parte tutta la comunicazione (portale di comunicazione e il personale che lo gestisce).
- Product Security Incident Response Team (PSIRT): un team di esperti responsabile, a livello globale o locale, dell'esecuzione del processo qui descritto.

---

2. Ruoli e responsabilità

Gestione della qualità e della conformità:

- Parte del personale dello SPOC responsabile delle segnalazioni in entrata e in uscita (a livello globale), comunicazione con i segnalanti.
- Coordinamento del PSIRT (a livello locale)
- Verifica degli aspetti legali
- Invio delle segnalazioni alle autorità (ENISA/CERT-Bund)

Il team di gestione della qualità ha stabilito apposite regole di sostituzione.

Product Security Incident Response Team (PSIRT):

- Categorizzazione, convalida, definizione delle priorità, coordinamento con i team di prodotto
- Comunicazione con i segnalanti e, se necessario, con le autorità/i CSIRT
- Pubblicazione di avvisi di sicurezza

I membri del PSIRT sono designati a livello globale e locale e sono coordinati dal team di gestione della qualità (QM).

Team di ingegneria (come parte del PSIRT):

- Analisi tecnica, correzione/mitigazione, test, pianificazione del rilascio
- Gestione di SBOM/informazioni sui componenti (se disponibili)

Ingegneria delle applicazioni (come parte del PSIRT):

- Coinvolgimento nella comunicazione con i clienti/soluzioni alternative/misure di mitigazione

Registrazione di prodotti e materiali (come parte del PSIRT):

- Fornisce, se necessario, le informazioni necessarie per la tracciabilità di vendite, acquisti, altri movimenti di materiale, scorte di magazzino e ordini in sospeso.

---

3. Canali di segnalazione (Vulnerability Intake)

Le segnalazioni possono essere inviate tramite:

- **Da parte dei clienti e di altri soggetti esterni**: SPOC/modulo web: https://www.alliedvision.com/it/company/legal-and-compliance/cybersecurity
- Da parte del personale interno: e-mail: quality@alliedvision.com (sezione a valle dello SPOC)

Informazioni richieste:

- Prodotto interessato (codice articolo, numero/i di serie)
- Descrizione della vulnerabilità e delle conseguenze
- Passaggi per la riproduzione / Proof of Concept (se possibile)
- Impatto sulla sicurezza osservato/previsto
- Contatto per ulteriori chiarimenti
- **Facoltativo**: log, screenshot, dettagli sull'exploitability

---

4. Safe Harbor / Dichiarazione di buona fede

Allied Vision si impegna a non intraprendere azioni legali nei confronti di chi segnala casi relativi a **ricerche sulla sicurezza condotte in buona fede**, a condizione che:

- effettuino solo test minimi e necessari,
- non esfiltrino, alterino o compromettano in modo permanente i dati,
- non ricorrano a tecniche di ingegneria sociale e/o phishing nei confronti dei dipendenti,
- non violino i diritti di terzi con i propri test,
- non rendano pubblica la vulnerabilità prima che sia stato concordato un calendario di coordinamento (vedi sezione 8),
- rispettino le leggi vigenti.

In caso di accesso involontario a dati personali: **interrompere immediatamente** l'operazione, non salvare né trasmettere i dati e informare Allied Vision tramite il canale di segnalazione sopra indicato.

Un comportamento scorretto da parte di chi effettua la segnalazione non esonera Allied Vision dall'obbligo di risolvere una vulnerabilità effettivamente esistente.

---

5. Panoramica del processo (end-to-end)

Catena di processo: Ricezione → Conferma → Classificazione → Convalida → Priorizzazione → Misure immediate → Piano d'azione e analisi approfondita delle cause alla radice → Risoluzione/Mitigazione → Verifica → Rilascio/Implementazione/Divulgazione di avvisi di sicurezza → Misure preventive e attività di follow-up.

5.1 Ricezione e conferma

- Il processo può essere avviato tramite:
    - Segnalazione del cliente (vedi punto 3)
    - Segnalazione interna (test di penetrazione, informazioni provenienti da banche dati pubbliche sulla sicurezza informatica come ENISA)
- Il reparto QM assegna un ID ticket e individua un referente.
- Il reparto QM conferma la ricezione al segnalante il prima possibile, indicando l'ID ticket e il referente

5.2 Classificazione

- Valutazione iniziale da parte del reparto QM (eventualmente con il supporto del team di ingegneria) per verificare se la segnalazione sia plausibile e rientri nell'ambito di applicazione.
  Possibili risultati: **valido/non valido (non riproducibile / fuori dall'ambito / duplicato).**
- In caso di risultato «non valido», il segnalante viene informato e, se necessario, gli vengono richieste ulteriori informazioni per una nuova valutazione. La pratica viene chiusa con motivazione una volta conclusa la comunicazione con il segnalante.

5.3 Convalida e definizione delle priorità (in base alla gravità)

- In caso di risultato "valido", la convalida viene proseguita dal team di ingegneria.
    - I criteri relativi allo "sfruttamento attivo di una vulnerabilità" o a un "incidente di sicurezza grave" si basano sulle definizioni dell'articolo 3 del CRA, punti 42 e 44.

Le segnalazioni convalidate vengono classificate in base alla priorità:

- **Critical** (tra cui: vulnerabilità sfruttata, esecuzione di codice remoto, bypass dell'autenticazione, sfruttabile su larga scala)
- **High** (il potenziale sfruttamento ha un impatto elevato)
- **Medium** (il potenziale sfruttamento ha un impatto limitato)
- **Low** (vulnerabilità non sfruttabile). In questi casi, la pratica viene chiusa e, se necessario, ulteriormente elaborata dal reparto di ingegneria nel processo di sviluppo senza fissare una scadenza.

5.4 Misure immediate

- Non appena viene convalidato lo sfruttamento attivo di una vulnerabilità o un grave incidente di sicurezza, il reparto QM lo segnala al CERT-BUND e all'ENISA entro e non oltre 24 ore dalla convalida. Ulteriori obblighi di segnalazione a CERT-Bund ed ENISA con relative scadenze: si veda la sezione 6.
- I segnalanti vengono informati dell'esito (con motivazione).
- In caso di livelli «Critical» e «High», viene pianificata l'ulteriore informazione delle parti interessate rilevanti (CERT-BUND, ENISA, segnalanti, clienti) e attuata secondo il piano documentato.

5.5 Piano d'azione e analisi approfondita delle cause alla radice

- Viene redatto un piano d'azione che comprende le fasi indicate di seguito, nonché l'informazione delle autorità, dei segnalanti e dei clienti.
- Se la causa alla radice dell'errore identificato non è ancora chiara, questa viene ora individuata.

5.6 Risoluzione e mitigazione

- Il team di ingegneri elabora una correzione o una soluzione alternativa.
- Qualora non sia possibile una correzione immediata: si ricorre alla **mitigazione** (configurazione, regola WAF, feature flag, limitazione della frequenza, ecc.).
- Le modifiche rilevanti per la sicurezza vengono sottoposte a una revisione di sicurezza e a test di regressione.

5.7 Verifica

- La correzione viene verificata rispetto al Proof of Concept (PoC); se possibile, si chiede a chi ha segnalato il problema di ripetere il test.
- Vengono individuate le versioni interessate e l'eventuale necessità di un downgrade.

5.8 Rilascio/Implementazione/Divulgazione di avvisi di sicurezza

- Una patch viene pubblicata sul sito web (vedi 3. SPOC).
- Le note di rilascio e le istruzioni per l'aggiornamento vengono inviate a chi ha segnalato il problema e pubblicate in generale sul sito web (vedi 3. SPOC).
- Se necessario, vengono pubblicati avvisi di sicurezza sul sito web (SPOC)

5.9 Misure preventive e attività successive

- Sulla base dell'analisi delle cause alla radice e di ulteriori conoscenze acquisite (lessons learned), se necessario, il reparto di ingegneria attua miglioramenti al ciclo di vita dello sviluppo sicuro del software (Secure Software Development Life Cycle) o altre misure preventive.
- Vengono aggiornati i modelli di minaccia, le linee guida per la codifica sicura e i casi di test.

---

6. Termini

Obblighi di segnalazione e rendicontazione nei confronti del CERT-Bund e dell'ENISA

Qualora, per i prodotti con elementi digitali rientranti nell'ambito di applicazione del Cyber Resilience Act (CRA) dell'UE, sia stato accertato lo sfruttamento attivo di una vulnerabilità o si sia verificato un grave incidente di sicurezza, ai sensi dell'articolo 14 del CRA sussistono termini di segnalazione vincolanti nei confronti del CERT-Bund e dell'ENISA, che Allied Vision si impegna a rispettare:

- Allerta precoce (Early Warning): entro 24 ore.
- Notifica (Notification): entro 72 ore, con una prima valutazione, il livello di gravità e, se del caso, gli indicatori di compromissione.

- Relazione finale (Final Report):
    - **Critical**: relazione finale entro e non oltre 14 giorni.
    - **Medium - High**: rapporto finale entro 14 giorni dalla disponibilità di una misura correttiva o di mitigazione, ma comunque entro un mese al massimo.
- Responsabile della segnalazione alle autorità: Quality and Compliance Management (SPOC), se necessario in coordinamento con i consulenti legali dell'azienda.
- Indipendentemente da ciò, permangono gli obblighi di segnalazione ai sensi degli articoli 33 e 34 del GDPR (72 ore), qualora siano coinvolti dati personali (cfr. sezione 4).

Inoltre, si applicano i seguenti **tempi di riferimento** (i tempi dipendono dal livello di criticità desumibile dalla segnalazione del cliente; in caso di forte sospetto di sfruttamento attivo con gravi conseguenze, i termini vengono abbreviati):

- **Conferma di ricezione:** ≤ 2 giorni lavorativi
- **Categorizzazione e convalida:**
- Se la criticità presunta è «high» o «critical»: ≤ 5 giorni lavorativi
- Se la criticità presunta è «low» o «medium»: ≤ 15 giorni lavorativi
- **Obiettivo per il completamento delle misure correttive:**
    - Critical: ≤ 15–30 giorni (o al più presto in caso di sfruttamento)
    - High: ≤ 60 giorni
    - Medium: ≤ 90 giorni
    - Low: in base al ciclo di rilascio, di norma ≤ 180 giorni

Se la correzione richiede più tempo: il PSIRT informa il segnalante fornendo una motivazione e un nuovo calendario.

---

7. Comunicazione e coordinamento

Con chi segnala le vulnerabilità:

- Aggiornamenti regolari (ogni 14 giorni in caso di vulnerabilità di livello "High" o "Critical", altrimenti mensili).
- Accordi chiari sulla tempistica di pubblicazione.

Con i clienti/il pubblico:

- Pubblicazione delle vulnerabilità sul sito web (vedi 3. SPOC).
- In caso di rischi significativi, viene pubblicato un Security Advisor (vedi 3. SPOC).
- L'Advisory contiene: descrizione, versioni interessate, impatto, punteggio secondo il Common Vulnerability Scoring System (CVSS), misure di mitigazione, versioni corrette.

Con enti esterni:

- Se necessario, segnalazione al CERT-BUND e all'ENISA secondo le disposizioni del regolamento (vedi 5.4).

Con i reparti interni:

- Comunicazione e documentazione all'interno del PSIRT tramite Jira.
- Comunicazione con la direzione aziendale tramite il reparto QM in caso di casi gravi.
- Coinvolgimento dei consulenti legali esterni tramite il reparto QM o la direzione aziendale, se necessario.

---

8. Regole di divulgazione (pubblicazione coordinata)

Principio: Allied Vision e chi segnala la vulnerabilità mirano a una pubblicazione coordinata non appena è disponibile una correzione o una misura di mitigazione efficace.

Standard:

- Pubblicazione entro e non oltre **90 giorni** dalla convalida, **o** prima se è disponibile una patch.
- È possibile una proroga se (a) la correzione è complessa, (b) l'ecosistema degli utenti richiede tempi di implementazione più lunghi, (c) non vi sono indicazioni di sfruttamento attivo.
- In caso di **sfruttamento attivo**, Allied Vision può emettere un avviso anticipato (anche in assenza di una correzione definitiva) per proteggere gli utenti.

Pubblicazione anticipata da parte di chi segnala la vulnerabilità:

Chiediamo a chi segnala la vulnerabilità di consultarci in caso di pubblicazione pianificata prima della scadenza prevista; in caso di pubblicazione non coordinata, daremo priorità alle misure di protezione e alla comunicazione.

Fanno comunque fede gli obblighi di segnalazione sopra indicati.

---

9. Gestione delle informazioni sensibili

- I dettagli, i proof of concept e le informazioni tecniche relative agli exploit vengono trattati secondo il principio del "need-to-know".
- L'accesso è riservato esclusivamente alle persone coinvolte nell'analisi e nella risoluzione del problema (in particolare il PSIRT)
- Archiviazione in sistemi protetti (sistema di ticketing con controllo degli accessi, crittografia).
- I dati sensibili vengono classificati secondo il sistema in vigore presso Allied Vision.
- I dati sensibili vengono cancellati non appena non sono più necessari e purché non vi siano disposizioni di legge che lo impediscano.

---

10. Classificazione delle vulnerabilità e identificatori

- A ogni segnalazione viene assegnato un ID interno, utilizzato per l'ulteriore elaborazione della pratica, comprese tutte le comunicazioni e la documentazione.
- Se del caso, viene richiesto/coordinato un "Common Vulnerabilities and Exposures" (CVE).
- Gli avvisi fanno riferimento alle versioni di correzione e, se del caso, al CVE.

---

11. Dipendenze / Componenti di terze parti

Se le vulnerabilità risiedono in componenti di terze parti:

- Il PSIRT coordina la gestione del problema con il fornitore/produttore del componente.
- La comunicazione ai clienti contiene indicazioni chiare sulle versioni interessate e sulle soluzioni alternative.
- Se il fornitore continua a non rispondere, il PSIRT adotta autonomamente misure di mitigazione.
    - Il fornitore viene sottoposto a una nuova valutazione; gli vengono comunicati il risultato della valutazione e le conseguenze che ne derivano (da tenere presente per i fornitori cinesi: in quel Paese la graduale eliminazione di un prodotto in base alle leggi dell'UE è soggetta a sanzioni).
    - In caso di rischio accertato/convalidato: procedere come descritto nella sezione 5.5 e seguenti.
    - In caso di rischio presunto: vengono effettuate ulteriori valutazioni con l'obiettivo di classificare e convalidare il rischio. Successivamente, procedere come descritto nella sezione 5.5 e seguenti.

---

12. Violazioni delle politiche e abusi

Allied Vision può rifiutare le segnalazioni qualora queste contengano:

- ricatto ("pay or disclose"); in tal caso, la segnalazione verrà inoltrata alle autorità giudiziarie competenti.
- sottrazione intenzionale di dati o interruzione del servizio,
- scansioni automatizzate su larga scala contro sistemi produttivi senza autorizzazione,
- ingegneria sociale.

Un comportamento scorretto da parte di chi effettua la segnalazione non esonera Allied Vision dall'obbligo di risolvere una vulnerabilità effettivamente esistente.

---

13. Controllo delle versioni, revisione e formazione

- Responsabile del presente documento: Responsabile PSIRT (QM).

- Revisione: almeno una volta all’anno oppure a seguito di un incidente grave o di una modifica del quadro normativo (Cyber Resilience Act).
- Formazione: per i membri del PSIRT in merito alla ricezione, alla gestione, all’escalation e alla riservatezza.
- Documentazione: nel sistema di gestione dei documenti dell’azienda (Q.Wiki).

Allegato A: Modello di conferma di ricezione (e-mail)

Oggetto: [ID ticket] Segnalazione di vulnerabilità – Ricezione confermata

Grazie per la sua segnalazione. Abbiamo registrato la segnalazione con l'ID **[ID ticket].**

Le faremo sapere entro e non oltre il **[data]** con una prima valutazione/convalida.

Può contattarci all'indirizzo quality@alliedvision.com.

Per la comunicazione di dati sensibili, la preghiamo di utilizzare S/Mime per la crittografia delle e-mail oppure di richiederci un accesso protetto.

Allegato B: Modello di avviso di sicurezza (per il sito web)

Titolo: [Prodotto] – [CVE-XXXX-YYYY] – [Impatto sintetico]
Data: [YYYY-MM-DD]
Gravità: [Critical/High/Medium/Low] (CVSS v4.0: [Punteggio], Vettore: [..])
Prodotti interessati: [Modelli/Rev. HW], [Versioni firmware],
Sintesi: [2–4 frasi]
Dettagli tecnici: [quanto basta, il meno possibile]
Misure di mitigazione/soluzioni alternative: [passaggi]
Correzione: [versione/data di distribuzione OTA/aggiornamento manuale]
Cronologia: [segnalato/analizzato/risolto/divulgato] (facoltativo)

Allegato C: Modello di aggiornamento sullo stato (e-mail)

Oggetto: [ID ticket] Segnalazione di vulnerabilità – Aggiornamento sullo stato

La informiamo in merito allo stato della Sua segnalazione [ID ticket]. Stato attuale: [Stato]. Prossimo aggiornamento previsto: [Data]. Per eventuali domande, può contattarci all'indirizzo quality@alliedvision.com.

Allegato D: Modello di rifiuto (e-mail)

Oggetto: [ID ticket] Segnalazione di vulnerabilità – Risposta

La ringraziamo per la sua segnalazione [ID ticket]. Dopo averla esaminata, classifichiamo la segnalazione come [Non riproducibile / Fuori ambito / Duplicata]. Motivazione: [Motivazione]. Qualora dovessero emergere nuovi elementi, potrà inviare nuovamente la segnalazione.

Motivazione: [Motivazione]. Qualora dovessero emergere nuovi elementi, potrà inviare nuovamente la segnalazione.