Vulnerability Disclosure Policy
Allineata al Regolamento (UE) 2024/2847
Cyber Resilience Act (CRA)

1 Indice

1 Indice 1
2 Scopo 2
3 Ambito di applicazione 2
3.1 Prodotti considerati nell'ambito della Policy 2
3.1.1 Autorizzazione per test volontari di vulnerabilità 3
4 Definizioni principali 3
5 Come segnalare una vulnerabilità o un incidente 4
5.1 Trattamento dei dati personali del segnalante 5
6 Processo interno di gestione (PSIRT) 5
6.1 Obblighi e tempistiche di segnalazione a ENISA (art. 14 CRA) 5
7 Divulgazione pubblica coordinata 6
8 Impegno di "Safe Harbor" 7
9 Revisione e aggiornamento della Policy 7
10 Contatti 7

2 Scopo

La presente Vulnerability Disclosure Policy ("Policy" o "VDP") definisce le modalità con cui **OCME Srl** (di seguito "l'Azienda") riceve, valuta, gestisce e comunica le segnalazioni di vulnerabilità di sicurezza informatica relative ai propri prodotti con elementi digitali, in particolare macchine, sistemi di automazione e relativi componenti software/firmware.

La Policy è stata predisposta in conformità al Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio europeo (Cyber Resilience Act, "CRA"), che impone ai fabbricanti di prodotti con elementi digitali l'adozione di un processo di gestione delle vulnerabilità durante l'intero ciclo di vita del prodotto, incluso un canale di divulgazione coordinata delle vulnerabilità (art. 13) e obblighi di segnalazione tempestiva a ENISA e al CSIRT designato in caso di vulnerabilità attivamente sfruttate o incidenti gravi (art. 14).

L'Azienda si impegna a non intraprendere azioni legali nei confronti di chi segnala, in buona fede e nel rispetto della presente Policy, una potenziale vulnerabilità riscontrata nei prodotti dell'Azienda.

3 Ambito di applicazione

La Policy si applica a tutti i prodotti con elementi digitali immessi sul mercato dall'Azienda, comprese le macchine e i sistemi di automazione dotati di componenti elettronici, connettività di rete o interfacce di comunicazione remota. Le seguenti sezioni chiariscono cosa rientra e cosa non rientra nel perimetro della Policy.

3.1 Prodotti considerati nell'ambito della Policy

Sono sottoposti alla presente Policy tutti i prodotti realizzati dall'Azienda e offerti ai propri clienti inclusi:

- intere macchine automatiche, in particolare con riferimento a riempitrici (modelli: Libra), sistemi di confezionamento secondario e di asservimento (modelli: Vega; Altair; Cygnus; Chamaeleon; Scorpius), sistemi di paletizzazione e depallettizzazione (modelli: Pegasus; Perseus; Orion; Ares; Mizar; Dorado), decassettatrici e incassettatrici (modelli: Leo), sistemi di movimentazione tradizionale (Trasporti prodotto in packaging primario, Trasporti prodotto in packaging secondario, Trasporti palette) e sistemi di movimentazione logistica mediante veicoli automatici (modelli: Auriga);
- prodotti software di supervisione, in particolare: Soluzioni di etichettatura palette, Sistema di avviamento remoto delle linee (Job Executor), Sistemi di supervisione di impianto.

Sono invece da escludersi dalla presente Policy tutti quei sistemi che non sono realizzati dall'Azienda o che non sono integrati all'interno delle soluzioni proposte dall'Azienda. A titolo esemplificativo, ma non esaustivo, sono esclusi i sistemi informativi aziendali del cliente non correlati ai prodotti dell'Azienda, come sistemi ERP,

MES, e in generale tutti i sistemi di livello IT, nonché tutto ciò che è fornito da terzi parti non rientrante nello scopo di fornitura dell'Azienda.

3.1.1 Autorizzazione per test volontari di vulnerabilità

L'esecuzione di attività di verifica, analisi, valutazione o testing della sicurezza informatica sui prodotti dell'Azienda rientranti nell'ambito di applicazione della presente Policy non è consentita, salvo preventiva autorizzazione espressa rilasciata dall'Azienda mediante accordo scritto che disciplini le modalità, i limiti e le condizioni delle attività autorizzate.

L'Azienda si riserva il diritto di richiedere la presenza, in modalità fisica o da remoto, di un proprio rappresentante incaricato per tutta la durata delle verifiche.

4 Definizioni principali

- Prodotto con elementi digitali: prodotto software o hardware, e le relative soluzioni di trattamento remoto dei dati, compresi i componenti software o hardware immessi separatamente sul mercato, ai sensi dell'art. 3, punto 1, del CRA
- Fabbricante: persona fisica o giuridica che sviluppa o fabbrica prodotti con elementi digitali, o che li fa progettare, sviluppare o fabbricare, e li commercializza con il proprio nome o marchio, a titolo oneroso, gratuito o mediante altra forma di monetizzazione, ai sensi dell'art. 3, punto 13, del CRA. Ai fini della presente Policy, l'Azienda opera in qualità di fabbricante rispetto ai prodotti di cui alla Sezione 3.1.
- Vulnerabilità: debolezza, suscettibilità o difetto di un prodotto con elementi digitali che può essere sfruttata da una minaccia informatica.
- Vulnerabilità attivamente sfruttata: vulnerabilità per la quale esiste evidenza credibile che un attore malevolo ne stia sfruttando l'esistenza in un prodotto senza il consenso del proprietario del sistema.
- Incidente grave: evento con impatto negativo effettivo sulla sicurezza di un prodotto con elementi digitali, secondo i criteri definiti dalla Commissione europea/ENISA ai sensi dell'art. 14 CRA.
- Divulgazione coordinata delle vulnerabilità (CVD): processo strutturato tramite il quale le vulnerabilità sono segnalate al fabbricante in modo da consentirne la diagnosi e la remediation prima della divulgazione pubblica dei dettagli.
- PSIRT (Product Security Incident Response Team): team interno all'Azienda responsabile della ricezione, valutazione e gestione delle segnalazioni di vulnerabilità e degli incidenti di sicurezza sui prodotti.
- CSIRT designato: Computer Security Incident Response Team nazionale indicato quale coordinatore ai sensi del CRA per la ricezione delle notifiche, in raccordo con ENISA.

5 Come segnalare una vulnerabilità o un incidente

Le segnalazioni possono essere inviate attraverso il seguente canale dedicato predisposto dal PSIRT:

- E-mail: cra.compliance@ocme.com

Fermo restando il canale di contatto sopra indicato, restano validi ed utilizzabili anche gli ulteriori canali di comunicazione abitualmente impiegati dai clienti nei rapporti con l'Azienda. Ai sensi delle procedure interne di gestione delle segnalazioni, qualsiasi comunicazione, segnalazione o richiesta ricevuta attraverso canali diversi da quello dedicato saranno comunque prese in carico e gestite secondo i medesimi processi applicabili alle segnalazioni pervenute tramite il canale ufficiale, garantendo l'applicazione dei medesimi processi di gestione, valutazione e riscontro.

Tuttavia, al fine di garantire un trattamento corretto ed efficace delle segnalazioni di vulnerabilità, i soggetti segnalanti sono invitati a utilizzare il canale ufficiale sopra indicato. Per le segnalazioni ricevute tramite canali diversi, i tempi previsti dalla presente Policy, e le relative attività operative, decorrono dalla data in cui la segnalazione viene formalmente registrata e resa disponibile al PSIRT attraverso il processo interno di inoltro previsto dall'Azienda. L'Azienda non garantisce il rispetto delle tempistiche previste dalla presente Policy per il periodo intercorrente tra la ricezione della segnalazione su un canale non dedicato e la sua formale presa in carico da parte del PSIRT.

Al fine di consentire una corretta valutazione e gestione della segnalazione, il segnalante è invitato a fornire le seguenti informazioni minime:

1. Nome cliente, stabilimento produttivo e linea di produzione presso cui è installata o utilizzata la macchina o il software oggetto della segnalazione
2. Prodotto, modello e numero di serie della macchina o del software oggetto di segnalazione, riportato sulla targa CE applicata. Ad esempio:
   OCME Altair HT, serial number 1100045A01
3. Tipo di notifica: ovvero se si tratta di segnalazione di una vulnerabilità attivamente sfruttata, o il report di un incidente grave di sicurezza informatica
4. Descrizione tecnica della vulnerabilità o dell'incidente segnalato, comprensiva, ove disponibile, della relativa classificazione (ad esempio CWE).
5. Informazioni e passaggi necessari per la riproduzione della vulnerabilità o per la comprensione dell'evento segnalato, se noti al momento della segnalazione.
6. Log, evidenze tecniche, screenshot o altra documentazione pertinente disponibile
7. Valutazione dell'impatto potenziale o osservato in termini di riservatezza, integrità, disponibilità dei dati e dei sistemi.
8. Eventuali indicatori di sfruttamento attivo già osservati
9. Recapiti del segnalante, preferibilmente un indirizzo e-mail, per consentire eventuali richieste di chiarimento e le successive comunicazioni relative alla gestione della segnalazione

Qualora la segnalazione risulti incompleta, inesatta o non contenga le informazioni minime necessarie per la sua valutazione tecnica, l'Azienda potrà richiedere al segnalante integrazioni o chiarimenti. La mancanza delle informazioni essenziali può comportare ritardi nelle attività di analisi, classificazione e gestione della segnalazione.

5.1 Trattamento dei dati personali del segnalante

I dati personali eventualmente forniti dal segnalante nell'ambito di una segnalazione (a titolo esemplificativo, nome e recapiti di contatto) sono trattati dall'Azienda, in qualità di titolare del trattamento, esclusivamente per le finalità di gestione, valutazione e riscontro della segnalazione stessa, in conformità al Regolamento (UE) 2016/679 (GDPR) e alla normativa nazionale applicabile in materia di protezione dei dati personali. Per maggiori informazioni sulle modalità di trattamento, sui diritti dell'interessato e sui tempi di conservazione, si rimanda all'informativa privacy dell'Azienda.

6 Processo interno di gestione (PSIRT)

Il PSIRT gestisce ogni segnalazione secondo un processo strutturato che comprende le seguenti fasi:

1. Ricezione e registrazione della segnalazione nel sistema di tracciamento interno.
2. Triage iniziale: verifica di validità, pertinenza con la presente Policy e identificazione dei prodotti/versioni coinvolti.
3. Comunicazione al segnalante dell'esito delle verifiche iniziali ed eventuale richiesta di ulteriori informazioni.
4. Determinazione se la vulnerabilità risulti attivamente sfruttata o riconducibile a un incidente grave ai sensi dell'art. 14 CRA, con conseguente attivazione del workflow di notifica a ENISA/CSIRT descritto alla Sezione 6.1.
5. Identificazione della misura correttiva (patch, aggiornamento firmware, mitigazione compensativa).
6. Comunicazione ai clienti/utenti interessati, eventualmente anche tramite security advisory pubblicata sul sito web, con indicazioni sulle azioni da intraprendere.
7. Chiusura della segnalazione e, se concordata, divulgazione pubblica coordinata.
8. Analisi post-incidente (lessons learned) e aggiornamento dei processi, ove necessario.

6.1 Obblighi e tempistiche di segnalazione a ENISA (art. 14 CRA)

Quando una vulnerabilità gestita dal PSIRT risulta attivamente sfruttata, oppure si verifica un incidente grave che incide su un prodotto con elementi digitali, l'Azienda, in qualità di fabbricante, è tenuta a notificare ENISA attraverso la piattaforma unica di segnalazione istituita ai sensi dell'art. 16 CRA, rispettando le seguenti tempistiche:

Termine	Adempimento	Contenuto minimo
Entro 24 ore	Early warning notification	Notifica preliminare a ENISA/CSIRT designato tramite il punto di contatto unico. È comunicata la natura dello sfruttamento attivo o dell'incidente grave, prodotto/i coinvolti, Stati membri potenzialmente interessati (in questa fase le informazioni possono essere ancora parzialmente incomplete).
Entro 72 ore	Notifica di follow-up (vulnerability/incident notification)	Aggiornamento della notifica iniziale con informazioni disponibili su gravità, impatto, indicatori di compromissione e, se note, le misure correttive o mitigative già adottate o adottabili nel breve termine.
Entro 14 giorni dalla disponibilità della misura correttiva (vulnerabilità)	Rapporto finale	Descrizione dettagliata della vulnerabilità (causa, gravità, CVSS), conferma dell'avvenuta remediation e, se pertinente, misure di mitigazione messe a disposizione degli utenti.
Entro 1 mese dalla notifica iniziale (incidente grave)	Rapporto finale su incidente grave	Descrizione dell'incidente, causa scatenante, misure correttive applicate e impatto su parco macchine installate, ove rilevante.

L'obbligo di notifica delle vulnerabilità attivamente sfruttate e degli incidenti gravi ai sensi dell'art. 14 CRA si applica a decorrere dall'11 settembre 2026.

Il PSIRT mantiene una procedura operativa dedicata a garantire il rispetto di tali termini fin dalla data di entrata in vigore dell'obbligo.

7 Divulgazione pubblica coordinata

Qualora non sia possibile allertare tempestivamente e puntualmente tutti i soggetti interessati dalla medesima vulnerabilità attivamente sfruttata, o che possono incorrere in analoghi incidenti di sicurezza gravi, le attività di mitigazione vengono comunicate pubblicamente attraverso security advisory rese disponibili sul portale aziendale all'indirizzo

https://www.ocme.com/en/security-advisories.php

In ogni caso, la data di divulgazione pubblica è concordata con il segnalante, tenendo conto dei tempi necessari allo sviluppo e alla distribuzione della correzione che, nei settori in cui opera l'Azienda, può richiedere tempistiche estese. L'Azienda si impegna comunque a non ritardare la divulgazione oltre quanto strettamente necessario per informare e mettere in sicurezza il parco macchine e software installato.

8 Impegno di “Safe Harbor”

L'Azienda considera lecita, ai sensi della presente Policy, l'attività di segnalazione condotta in buona fede quando:

- le vulnerabilità identificate nel prodotto commercializzato dall’Azienda sono tempestivamente comunicate tramite i canali indicati alla Sezione 5
- le vulnerabilità non sono divulgate pubblicamente prima della data di divulgazione coordinata concordata con il PSIRT dell’Azienda.

Nel rispetto di tali condizioni, l'Azienda non promuoverà azioni legali civili o penali nei confronti del segnalante in relazione alla segnalazione svolta.

È fatto divieto di attuare comportamenti estorsivi, intimidatori o comunque non conformi ai principi di correttezza e buona fede. Il segnalante non dovrà richiedere, sollecitare o pretendere premi, compensi economici, benefici o altre forme di corrispettivo non espressamente concordate per iscritto con l’Azienda prima dell'esecuzione delle attività di ricerca o segnalazione. Inoltre, il segnalante si impegna a non trasmettere ripetutamente la medesima segnalazione, né a utilizzare indirizzi e-mail diversi o altre modalità finalizzate a far apparire la segnalazione come proveniente da soggetti distinti.

9 Revisione e aggiornamento della Policy

La presente Policy è riesaminata con cadenza annuale, o a seguito di modifiche significative del quadro normativo applicabile (incluse eventuali linee guida attuative di ENISA e della Commissione europea relative al CRA), e in ogni caso a seguito di lezioni apprese da incidenti gestiti dal PSIRT.

10 Contatti

- PSIRT: cra.compliance@ocme.com
- Sito web Advisories: https://www.ocme.com/en/security-advisories

- Sede legale: OCME Srl, via del Popolo 20/A – 43122 Parma (Italy)