Politica di Divulgazione Coordinata delle Vulnerabilità (CVD Policy)

FEC Italia S.r.l.
Via Spoleto 4, 33010 Tavagnacco (UD), Italia
www.fecpos.it · info@fecpos.it

Codice documento: **FEC-CVD-001** · *Versione 1.0* · *In vigore da: [11 Settembre 2026]*

Riferimenti normativi: Reg. (UE) 2024/2847 (Cyber Resilience Act), Allegato I Parte II punto 5; Allegato II punto 2.

1. Premessa

FEC Italia S.r.l. ("FEC") considera la sicurezza dei propri prodotti con elementi digitali una priorità. Riconosciamo il ruolo essenziale della comunità di ricerca sulla sicurezza e accogliamo segnalazioni di vulnerabilità nei nostri prodotti, impegnandoci a trattarle in modo trasparente, professionale e coordinato.

La presente policy descrive le regole con cui FEC riceve, gestisce e divulga le segnalazioni di vulnerabilità ricevute da ricercatori, clienti, fornitori, autorità competenti e CSIRT.

2. Ambito (Scope)

La policy si applica a tutti i prodotti hardware con elementi digitali fabbricati e/o commercializzati da FEC Italia S.r.l., ovunque essi siano stati immessi sul mercato nell'Unione Europea, includendo le linee di prodotto correnti e future.

Per ciascun prodotto, l'ambito copre:

- Hardware integrato (motherboard, firmware UEFI/BIOS, alimentatore, componenti wireless e altri sottosistemi forniti da FEC)
- Immagine sistema operativo installata di fabbrica da FEC
- Firmware e driver distribuiti da FEC tramite i canali ufficiali

Sono esplicitamente fuori scope:

- Applicazioni software installate dal cliente sul prodotto dopo la consegna
- Componenti hardware o software di terze parti non integrati direttamente da FEC nel prodotto

finito

- Vulnerabilità in prodotti di marche diverse rivendute da FEC o partner senza integrazione tecnica FEC
- Attacchi che richiedono accesso fisico non autorizzato al dispositivo (es. furto, manomissione hardware)
- Attacchi di social engineering verso il personale FEC o dei clienti
- Vulnerabilità denial-of-service che richiedono volumi di traffico anomali
- Vulnerabilità puramente teoriche senza prova di sfruttabilità pratica

In caso di dubbio sull'appartenenza di un prodotto allo scope, FEC invita a inviare comunque la segnalazione: confermeremo o smentiremo l'appartenenza allo scope in fase di triage.

3. Come segnalare una vulnerabilità

Le segnalazioni vanno inviate a:

Email: supporto@fecpos.it

Oggetto obbligatorio: [CVD] <breve descrizione>

Lingue accettate: italiano, inglese

Per comunicazioni cifrate è disponibile chiave PGP su richiesta a supporto@fecpos.it.

Informazioni da includere nella segnalazione:

- Descrizione tecnica della vulnerabilità
- Prodotto e versione interessati (linea di prodotto, modello commerciale, versione hardware, versione BIOS/firmware/OS se nota)
- Passi di riproduzione dettagliati
- Impatto stimato e scenario di sfruttamento
- Eventuale CVSS calcolato dal ricercatore
- Eventuale codice di prova o screenshot (preferibilmente trasmessi cifrati)
- Contatto di ritorno del ricercatore (email)

4. Tempistiche di risposta

FEC si impegna a rispettare le seguenti tempistiche per ogni segnalazione ricevuta:

Fase	Tempo massimo
Conferma di ricezione della segnalazione	5 giorni lavorativi
Valutazione iniziale (triage) e classificazione di	15 giorni lavorativi

gravità	
Aggiornamenti periodici al ricercatore sullo stato	Almeno ogni 30 giorni
Coordinamento sulla data di disclosure pubblica	Almeno 30 giorni prima della pubblicazione

Le segnalazioni sono trattate secondo le procedure interne FEC di gestione delle vulnerabilità conformemente al Reg. (UE) 2024/2847, Allegato I Parte II.

5. Divulgazione coordinata

FEC adotta un approccio di divulgazione coordinata delle vulnerabilità, in conformità con gli standard ISO/IEC 29147 e 30111:

- La divulgazione pubblica di una vulnerabilità avviene dopo che FEC ha reso disponibile la patch correttiva o, in casi eccezionali, dopo un periodo concordato con il ricercatore.
- Periodo standard di coordinamento: 90 giorni dalla conferma della vulnerabilità da parte di FEC. Periodi diversi possono essere concordati per vulnerabilità di particolare complessità tecnica o impatto.
- Per vulnerabilità attivamente sfruttate che presentano rischio elevato, FEC può anticipare la divulgazione e procederà alle notifiche obbligatorie a CSIRT/ENISA ai sensi dell'Art. 14 del Reg. (UE) 2024/2847.

6. Safe Harbor (salvaguardia)

FEC si impegna a non avviare azioni legali contro ricercatori che segnalino vulnerabilità in buona fede, a condizione che il ricercatore:

- Limiti la propria attività di test a quanto strettamente necessario per identificare e dimostrare la vulnerabilità
- Non causi danni a sistemi, dati o utenti
- Non acceda, modifichi, copi né distribuisca dati personali o riservati di clienti FEC o di terzi
- Non sfrutti la vulnerabilità per fini diversi dalla segnalazione
- Rispetti i tempi di disclosure coordinata definiti nella sezione 5
- Non divulghi pubblicamente la vulnerabilità prima che FEC abbia avuto la possibilità di valutarla e rilasciare la correzione

Le attività di ricerca conformi alla presente policy sono considerate autorizzate da FEC ai fini delle disposizioni del Reg. (UE) 2024/2847 e della normativa nazionale applicabile (es. art. 615-ter c.p.).

7. Riconoscimento

Salvo richiesta contraria del ricercatore, FEC riconosce pubblicamente il contributo di chi segnala

vulnerabilità includendone il nome (o pseudonimo) nell'advisory di sicurezza rilasciato al momento del fix.

FEC non offre programmi di bug bounty con compensazione economica.

8. Riservatezza

Le informazioni contenute nelle segnalazioni di vulnerabilità sono trattate come informazioni riservate da FEC fino al rilascio del fix e della relativa divulgazione pubblica coordinata, salvo obblighi normativi di notifica (es. CSIRT/ENISA ai sensi dell'Art. 14 CRA).

9. Contatti

Canale	Recapito
Email CVD / sicurezza	supporto@fecpos.it
Sito web	www.fecpos.it
Telefono	+39 0432 14 37 070
Indirizzo postale	FEC Italia S.r.l., Via Spoleto 4, 33010 Tavagnacco (UD), Italia

Direzione FEC Italia · Codice: FEC-CVD-001 · Aggiornato al: 15/05/2026