1) Finalità

Extrema si impegna a gestire in modo responsabile e coordinato le vulnerabilità di sicurezza eventualmente individuate nei propri prodotti con elementi digitali e nei relativi componenti software.

La presente politica definisce le modalità con cui è possibile segnalare a Extrema una potenziale vulnerabilità e il processo adottato per la sua valutazione, gestione e, ove necessario, risoluzione.

2) Chi può effettuare una segnalazione

Le potenziali vulnerabilità possono essere segnalate da qualsiasi persona fisica, o giuridica che ne venga a conoscenza, indipendentemente dal fatto che abbia o meno un rapporto contrattuale o commerciale con Extrema.
Sono pertanto, a titolo esemplificativo e non esaustivo, possibili segnalanti:

- rivenditori e distributori;
- installatori e manutentori;
- utilizzatori dei prodotti;
- ricercatori di sicurezza informatica;
- fornitori di componenti o servizi;
- società specializzate in cybersecurity;
- enti o organizzazioni che individuino una potenziale vulnerabilità.

3) Come segnalare una vulnerabilità

Le segnalazioni devono essere trasmesse al seguente punto di contatto:
Security contact: [security@Extrema.it]
La segnalazione dovrebbe contenere, ove disponibili:

- identificazione del prodotto interessato;
- versione del prodotto, del firmware o del software interessato;
- descrizione della potenziale vulnerabilità;
- condizioni necessarie per riprodurre il problema;
- eventuali prove tecniche o informazioni utili alla verifica;
- eventuali conseguenze sulla sicurezza;
- recapito del segnalante, se desidera essere ricontattato.

Non è necessario fornire informazioni che il segnalante non possiede o che non è ragionevolmente in grado di ottenere.

4) Tutela del segnalatore

Extrema non intraprenderà azioni legali nei confronti di chi segnala vulnerabilità in buona fede e nel rispetto della presente Politica, a condizione che le attività di ricerca e segnalazione non comportino violazioni della privacy, distruzione o alterazione dei dati, né interruzioni o compromissioni della disponibilità dei servizi.

5) Gestione delle segnalazioni

Extrema valuterà le segnalazioni ricevute e, ove necessario, procederà alla verifica tecnica della vulnerabilità, alla valutazione del rischio e all'individuazione delle opportune misure correttive o di mitigazione.
Quando appropriato, Extrema manterrà un dialogo con il segnalante durante il processo di analisi e gestione della vulnerabilità.

6) Divulgazione coordinata

Extrema applica un processo di divulgazione coordinata delle vulnerabilità (Coordinated Vulnerability Disclosure – CVD), finalizzato a consentire l'analisi e la risoluzione delle vulnerabilità prima della divulgazione pubblica di informazioni tecniche che potrebbero facilitare lo sfruttamento della vulnerabilità.
Le informazioni relative a una vulnerabilità saranno condivise con le parti interessate secondo il principio di necessità e tenendo conto del livello di rischio e delle esigenze di sicurezza.

7) Comunicazioni agli utilizzatori

Qualora una vulnerabilità richieda un intervento da parte degli utilizzatori, degli installatori, o dei soggetti incaricati della manutenzione, Extrema fornirà, ove applicabile, le necessarie informazioni e istruzioni e renderà disponibili le opportune misure correttive o di mitigazione.

8) Segnalazioni relative a prodotti di terzi

Qualora la segnalazione riguardi esclusivamente un componente o prodotto di terzi integrato nel prodotto Extrema, sarà Extrema stessa a valutare la segnalazione e, ove appropriato, collaborerà con il relativo fornitore per la gestione della vulnerabilità.

9) Contatti

Per le segnalazioni di vulnerabilità:
E-mail: security@extrema.it
Per richieste di assistenza tecnica, manutenzione o garanzia utilizzare invece i normali canali di assistenza Extrema.