

1) Finalité

Extrema s'engage à gérer de manière responsable et coordonnée les vulnérabilités de sécurité susceptibles d'être identifiées dans ses produits comportant des éléments numériques et dans leurs composants logiciels associés. La présente politique définit les modalités selon lesquelles une vulnérabilité potentielle peut être signalée à Extrema, ainsi que le processus adopté pour son évaluation, sa gestion et, le cas échéant, sa résolution.

2) Qui peut effectuer un signalement

Toute personne physique ou morale ayant connaissance d'une vulnérabilité potentielle peut la signaler, qu'elle entretienne ou non une relation contractuelle ou commerciale avec Extrema.

À titre d'exemple et sans que cette liste soit exhaustive, les personnes ou entités susceptibles d'effectuer un signalement comprennent :

- revendeurs et distributeurs ;
- installateurs et techniciens de maintenance ;
- utilisateurs des produits ;
- chercheurs en sécurité informatique ;
- fournisseurs de composants ou de services ;
- entreprises spécialisées en cybersécurité ;
- organismes ou organisations ayant identifié une vulnérabilité potentielle.

3) Comment signaler une vulnérabilité

Les signalements doivent être adressés au point de contact suivant :

Contact sécurité : [security@Extrema.it]

Le signalement devrait contenir, lorsque ces informations sont disponibles :

- identification du produit concerné ;
- version du produit, du micrologiciel ou du logiciel concerné ;
- description de la vulnérabilité potentielle ;
- conditions nécessaires pour reproduire le problème ;
- éventuels éléments de preuve techniques ou informations utiles à la vérification ;
- éventuelles conséquences en matière de sécurité ;
- coordonnées du déclarant, s'il souhaite être recontacté.

Il n'est pas nécessaire de fournir des informations que le déclarant ne possède pas ou qu'il n'est pas raisonnablement en mesure d'obtenir.

4) Protection du déclarant

Extrema n'engagera pas d'action en justice à l'encontre des personnes qui signalent des vulnérabilités de bonne foi et dans le respect de la présente Politique, à condition que les activités de recherche et de signalement n'entraînent pas d'atteinte à la vie privée, de destruction ou d'altération de données, ni d'interruption ou d'atteinte à la disponibilité des services.

5) Gestion des signalements

Extrema évaluera les signalements reçus et, le cas échéant, procédera à la vérification technique de la vulnérabilité, à l'évaluation des risques et à l'identification des mesures correctives ou d'atténuation appropriées. Lorsque cela est approprié, Extrema maintiendra un dialogue avec le déclarant pendant le processus d'analyse et de gestion de la vulnérabilité.

6) Divulgence coordonnée

Extrema applique un processus de divulgation coordonnée des vulnérabilités (Coordinated Vulnerability Disclosure – CVD), visant à permettre l'analyse et la résolution des vulnérabilités avant la divulgation publique d'informations techniques susceptibles de faciliter leur exploitation. Les informations relatives à une vulnérabilité seront communiquées aux parties concernées selon le principe du besoin d'en connaître, en tenant compte du niveau de risque et des exigences de sécurité.

7) Communications aux utilisateurs

Lorsqu'une vulnérabilité nécessite une intervention de la part des utilisateurs, des installateurs ou des personnes chargées de la maintenance, Extrema fournira, le cas échéant, les informations et instructions nécessaires et mettra à disposition les mesures correctives ou d'atténuation appropriées.

8) Signalements relatifs à des produits de tiers

Lorsqu'un signalement concerne exclusivement un composant ou un produit tiers intégré à un produit Extrema, Extrema évaluera elle-même le signalement et, le cas échéant, collaborera avec le fournisseur concerné pour la gestion de la vulnérabilité.

9) Contacts

Pour signaler une vulnérabilité :

E-mail : security@extrema.it security@extrema.it

Pour les demandes d'assistance technique, de maintenance ou de garantie, veuillez utiliser les canaux d'assistance habituels d'Extrema.