in progress - Politique de divulgation coordonnée des vulnérabilités - V2

Sercel R&D

24 July, 2026

Table of Contents

(Coordinated Vulnerability Disclosure – CVD)

1 1. Objet

La présente politique de divulgation coordonnée des vulnérabilités définit la manière dont Sercel reçoit, analyse, traite et divulgue les vulnérabilités de sécurité affectant ses produits.

Sercel, 16, rue de Bel Air - 44470 Carquefou - France : 02 40 30 11 81

Elle vise à :

- permettre le signalement responsable des vulnérabilités,
- protéger les clients et les utilisateurs,
- assurer une correction appropriée avant toute divulgation publique,
- respecter les exigences réglementaires applicables, notamment le **Cyber Resilience Act (CRA)**.

---

2 2. Périmètre

Cette politique s’applique à l’ensemble des produits matériels et logiciels développés, maintenus ou distribués par Sercel, qu’ils soient en phase de développement, de mise sur le marché ou de support.

Les exclusions portent sur :

- Produits matériels et logiciels utilisés en interne
- Prototypes non commercialisés

Un point important est l'analyse des modifications dites substantielles dans le cas des produits legacy.

Un **chercheur** est toute personne, qui analyse la sécurité des systèmes pour trouver des vulnérabilités.

- par exemple des experts cybersécurité, chercheurs indépendants, consultants, membres de la communauté sécurité

Un **découvreur** est toute personne, qui découvre une vulnérabilité. Il est encouragé à la signaler à **Sercel**.

- par exemple chercheurs, clients, partenaires, employés

---

3 3. Signalement des vulnérabilités

Les vulnérabilités peuvent être signalées de manière responsable via le point de contact suivant :

Canal	Coordonnées
📧 Email principal	Product_Security@sercel.com[1]
🌐 Formulaire web	À compléter — URL formulaire ou N/A (A définir dans la prochaine version)
🗣️ Langue acceptée	Français / Anglais

> ✅ *Conformément à l'Art.13§17 du Règlement (UE) 2024/2847 (CRA), Sercel désigne* Productsecurity@sercel.com[2]*comme point de contact unique officiel pour le signalement des vulnérabilités de ses produits comportant des éléments numériques.*
> *Le découvreur peut choisir son moyen de communication préféré. Ces moyens ne sont pas limités aux outils automatisés.*

Le signalement doit, dans la mesure du possible, inclure :

- une description de la vulnérabilité
- le produit et la version concernés
- les conditions d'exploitation connues
- tout élément technique utile à l'analyse

📌 Accessibilité publique et références réglementaires

La présente politique est publiquement accessible à l'adresse : À compléter — URL page sécurité sercel.com (a définir dans la prochaine version)

Elle est référencée dans :

- Les informations et instructions destinées aux utilisateurs de nos produits — Annexe II point 2 CRA
- La documentation technique de nos produits — Annexe VII CRA

1. mailto:Product_Security@sercel.com
2. mailto:Productsecurity@sercel.com

4 4. Engagements de traitement

Sercel s’engage à :

- accuser réception du signalement auprès du découvreur dans un délai raisonnable de l'ordre de 5 jours ouvrés,
- analyser la vulnérabilité signalée,
- évaluer son impact et son exploitabilité,
- définir et mettre en œuvre les mesures correctives appropriées,
- coordonner la divulgation de la vulnérabilité avec le découvreur.

Les délais de traitement et de correction peuvent varier en fonction de la nature et de la criticité de la vulnérabilité.

---

5 5. Divulgation coordonnée

La divulgation des informations relatives à une vulnérabilité est réalisée de manière coordonnée afin d’éviter l’exposition prématurée des utilisateurs à un risque de sécurité.

Sercel encourage les découvreurs à ne pas divulguer publiquement une vulnérabilité avant la mise à disposition d’un correctif ou d’une mesure d’atténuation appropriée, sauf accord préalable.

Le CSIRT coordinateur peut, sur demande du fabricant et pour des motifs justifiés de cybersécurité, retarder la diffusion de la notification jusqu'au consentement des parties, en en informant immédiatement l'ENISA. (article 16 CRA).

Néanmoins, Sercel s'engage à une divulgation dans un délai maximum de 90 jours, avec possibilité d'extension documentée si le correctif nécessite un déploiement terrain prolongé

6 6. Cadre réglementaire

Cette politique s’inscrit notamment dans le cadre :

- du **Cyber Resilience Act (Règlement UE 2024/2847)**,
- des bonnes pratiques de divulgation coordonnée des vulnérabilités.

---

7 7. Protection des chercheurs

Sercel n’engage aucune action juridique à l’encontre des chercheurs agissant de bonne foi, dans le respect de cette politique et des lois applicables.

---

8 8. Mise à jour de la politique

La présente politique peut être mise à jour périodiquement afin de tenir compte :

- de l'évolution des produits,
- des pratiques de sécurité,
- du cadre réglementaire.

Information	Détail	Signature
Responsable de la mise à jour	LAFUMA Stephan — Qualité LANÇON Philippe — Pilote CRA	☑ LAFUMA Stephan ☐ LANCON Philippe
Validateur	MADESCLAIRE Vincent — RSSI PETIT-LECLERC Céline — Adjointe Directeur Juridique DUBOUCHET Jérôme — Responsable Support Client et réparations global CARRE Nicolas — Directeur Pôle Digital Solutions TAUGAIN David — Responsable Pôle Systèmes embarqués FEUGERE Philippe — VP Produits & Services BENZARTI Serge — VP Qualité, Hse, Programs	☐ MADESCLAIRE Vincent ☐ PETIT-LECLERC Celine , GAUTIER Mathilde ☐ DUBOUCHET Jerome ☐ CARRE Nicolas ☐ TAUGAIN David ☐ FEUGERE Philippe ☑ BENZARTI Serge
Approbateur	DEJARDIN Romain — Direction	☐ DEJARDIN Romain
Fréquence de révision minimale	Une fois par an	
Dernière mise à jour	9 juil. 2026 — Version 2	

Information	Détail	Signature
Principales modifications	• Suppression de la référence au SLA (Service Level Agreement) qui est décrit dans le processus interne de gestion des vulnérabilités et des incidents. • Préciser que le temps de 5 jours est le temps d'accusé de réception auprès du découvreur (ce n'est pas une obligation CRA) • Nouveau mail de contact : Product_Security@sercel.com[3]	

3. mailto:Product_Security@sercel.com