SERCEL
A Viridien Business

COORDINATED VULNERABILITY DISCLOSURE POLICY

Sercel R&D

21 August, 2026

Table of Contents

1. Purpose

This Coordinated Vulnerability Disclosure Policy defines how Sercel organizes the receipt, analysis, handling and disclosure of security vulnerabilities affecting its products with digital elements.

Sercel, 16, rue de Bel Air - 44470 Carquefou - France: +33 2 40 30 11 81

It aims to:

- Enable responsible vulnerability reporting by any security researcher, customer, user or third party;
- Protect customers and users by limiting the risks of vulnerability exploitation;
- Ensure the implementation of appropriate corrective measures prior to any public disclosure where possible;
- Contribute to compliance with applicable cybersecurity regulatory requirements and, in particular, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), which requires manufacturers to establish and apply a coordinated vulnerability disclosure policy.

2. Scope

2.1. Scope

This policy applies to all hardware and software products with digital elements developed, maintained or distributed by Sercel, whose intended or reasonably foreseeable use involves a direct or indirect, logical or physical connection to a device or network, regardless of their lifecycle phase (development, market release, operation, support or corrective maintenance).

This policy also covers legacy products still in use or supported by Sercel. For these products, particular attention is paid to the analysis of substantial modifications that may affect their cybersecurity compliance and vulnerability exposure.

The following are excluded from the scope of this policy:

- Hardware and software products used exclusively internally by Sercel and not made available on the market;
- Non-commercialized prototypes not made available to customers or partners.

2.2. Definition of Disclosure Stakeholders

- **Security researcher**

Any person who analyzes the security of Sercel's products or systems in order to identify security vulnerabilities, such as cybersecurity experts, independent researchers, consultants or members of the cybersecurity community.

- **Vulnerability reporting party**

Any person who reports to Sercel a vulnerability affecting a Sercel product or service, whether a security researcher, customer, partner or employee. The reporting party is encouraged to report the vulnerability to **Sercel in accordance with this policy**.

---

3. Vulnerability Reporting

Vulnerabilities may be responsibly reported via the following contact point:

Channel	Details
Main Email	Product_Security@sercel.com[1]
Web Form	To be completed — Form URL or N/A (to be defined in next version)
Accepted languages	French / English

> In accordance with Article 13, paragraph 17, of Regulation (EU) 2024/2847 (Cyber Resilience Act), Sercel designates this email address as the official single point of contact for reporting vulnerabilities affecting its products with digital elements. The reporting party may use the communication channel of their choice to report a vulnerability. These means are not limited to automated tools.

[1]. mailto:Product_Security@sercel.com

Where possible, the report should include the following elements:

- A description of the vulnerability;
- Identification of the affected product (name, model) and, where applicable, the version;
- Known or suspected exploitation conditions;
- Any technical information useful for analysis.

Public accessibility and regulatory references

This policy is publicly accessible at Sercel Web Site : https://www.sercel.com/en/cyber-resilience-act

It is referenced in particular in:

- The information and instructions intended for product users, in accordance with Annex II, point 2 of Regulation (EU) 2024/2847;
- The technical documentation of products in accordance with Annex VII of Regulation (EU) 2024/2847.

4. Handling Commiments

Sercel implements a vulnerability management process compliant with the applicable cybersecurity requirements for products with digital elements and commits, for each report received, to:

- Acknowledging receipt of the report to the reporting party within a reasonable timeframe;
- Analyzing the reported vulnerability;
- Assessing its impact, severity and exploitability, in particular with regard to the security risks for products and their users;
- Defining and implementing appropriate corrective measures (e.g. patches, security updates, mitigation measures);
- Coordinating, where relevant, the disclosure of the vulnerability with the reporting party in order to limit the risks of exploitation prior to the availability of fixes.

Analysis, handling and remediation timelines may vary depending on the nature, complexity and severity of the vulnerability. Sercel endeavors, however, to prioritize vulnerabilities that are likely to be actively exploited or that present a significant risk to users.

In compliance with its regulatory obligations, Sercel:

- Notifies, where applicable, actively exploited vulnerabilities and serious incidents to the competent authorities, in accordance with the procedures and timelines set out in Regulation (EU) 2024/2847, in particular via the European Union Agency for Cybersecurity (ENISA) and national CSIRTs;
- Informs affected users of the vulnerability and the recommended security or mitigation measures as soon as possible, where necessary to reduce the risks of exploitation.

5. Coordinated Disclosure

The disclosure of information relating to a vulnerability is carried out in a coordinated manner in order to limit exploitation risks and avoid premature exposure of users to a security risk.

Sercel encourages security researchers and all reporting parties not to publicly disclose a vulnerability before a fix or appropriate mitigation measure is made available, unless prior agreement has been reached with Sercel.

In accordance with the framework provided for by Regulation (EU) 2024/2847, the coordinating CSIRT may, at the manufacturer's request and for justified cybersecurity reasons, delay the release of the vulnerability notification, subject to the consent of the parties concerned, and immediately informing the European Union Agency for Cybersecurity (ENISA).

Sercel commits, except in duly justified exceptional circumstances, to preparing and publishing a security advisory or equivalent communication describing the vulnerability, its impact and the recommended measures, within a reasonable timeframe from receipt of the report, where this is compatible with the implementation of a fix or mitigation measures.

Where remediation or operational deployment (in particular in the field) requires additional time, Sercel may extend this timeframe provided that:

- This extension is documented internally;
- The reporting party is informed of the reasons for this delay;
- Temporary mitigation measures are communicated to users where possible.

6. Regulatory Framework

This Coordinated Vulnerability Disclosure Policy is based in particular on:

- **Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act / CRA), which requires manufacturers of products with digital elements to establish vulnerability management processes and apply a coordinated vulnerability disclosure policy throughout the intended period of use of the products;**
- The European cybersecurity framework complementing the CRA, including in particular Directive (EU) 2022/2555 (NIS 2), which strengthens the security requirements for network and information systems and organizes cooperation between CSIRTs and national authorities, as well as incident and vulnerability notification mechanisms;
- Best practices for coordinated vulnerability disclosure (CVD), aimed at promoting responsible vulnerability reporting by security researchers, customers, partners and other stakeholders, and at organizing a progressive and coordinated disclosure that limits exploitation risks prior to the availability of corrective measures.

7. Protection of Researchers and Reporting Parties

Sercel recognizes the importance of the contributions of security researchers and vulnerability reporting parties to improving the cybersecurity of its products. Subject to compliance with this policy and applicable laws and regulations, Sercel:

- Will not take legal action against security researchers or reporting parties acting in good faith in the context of reporting a vulnerability affecting its products;
- Will refrain, under the same conditions, from requesting its partners or customers to take such actions against these researchers or reporting parties.

This protection does not, however, imply any tolerance for illegal activities, fraudulent or malicious behavior, or any act intentionally compromising the confidentiality, integrity or availability of the systems or data of customers, users or Sercel.

8. Policy Updates

This policy may be updated periodically to take into account:

- Product evolution;
- Security practices;
- The regulatory framework.

Information	Details
Last update	20 August 2026 - Version 2.1

SERCEL
A Viridien Business

SERCEL - FRANCE
16 rue de Bel Air
B.P. 30439 - 44474 CARQUEFOU Cedex
Téléphone : (33) 2 40 30 11 81
E-mail : sales.nantes@sercel.com
SAS au capital de 25 000 000 €
Siège Social : 16 rue de Bel Air - 44470 CARQUEFOU
378.040.497 R.C.S. Nantes Code APE 2651B

www.sercel.com