| Written by: | Checked by: | Approved by: |
|---|---|---|
| Anthony LAUMONNIER | Sébastien ARCHENY | Eric COTELLE |
| **Sign:** | **Sign:** | **Sign:** |
| 2026.03.11 | 2026/03/12 | 2026/03/18 |

# Table of contents

# 1. Introduction

The purpose of this Coordinated Vulnerability Disclosure (CVD) Policy is to establish Poclain's formal approach to identifying, reporting, assessing, and remediating security vulnerabilities affecting its Products with Digital Elements (PDEs).

This policy is a key component of Poclain's cybersecurity governance framework and supports compliance with the **EU Cyber Resilience Act (CRA)**, particularly requirements for:

- Continuous post-market vulnerability handling
- Secure product lifecycle management
- Mandatory reporting of actively exploited vulnerabilities and severe security incidents
- Cooperation with CSIRTs* and ENISA

Poclain implements structured and documented processes throughout the entire lifecycle of its products to:

- Ensure efficient vulnerability intake and triage
- Assess exploitability, safety, and operational impacts
- Deploy corrective actions in a reasonable timeframe
- Inform users about risks and mitigation when necessary
- Meet CRA obligations regarding vulnerability and incident reporting

This policy describes how Poclain collaborates with security researchers, customers, integrators, and partners to ensure vulnerabilities are disclosed responsibly and safely, preventing premature exposure and reducing malicious exploitation risks.

Poclain is committed to transparency, confidentiality, and regulatory compliance, ensuring its products remain secure, resilient, and trustworthy throughout their operational lifecycle.

ℹ Note: CSIRT FR for Poclain is ANSSI.

## 2. Scope & Applicability

This Coordinated Vulnerability Disclosure (CVD) Policy applies to all individuals and organizations involved in identifying, reporting, or managing security vulnerabilities related to **Poclain Products with Digital Elements (PDEs)** and associated digital services.

It covers the following stakeholders:

- **Independent security researchers** performing good-faith testing.
- **Customers, operators, and system integrators** deploying Poclain technologies.
- **Partners, suppliers, and third-party developers** interacting with Poclain hardware, embedded software, or cloud components.
- **Any stakeholder** who becomes aware of a potential vulnerability affecting Poclain products or digital infrastructure.

For the purposes of this policy, **"Product"** refers to any Poclain component containing digital functionality, including but not limited to:
Embedded software, firmware, ECUs, bootloaders, communication interfaces, cloud services, backend APIs, development tools, and associated documentation.

This policy applies to **all Poclain PDEs, and digital services covered by the EU Cyber Resilience Act (CRA)**.
In particular:

- **Mandatory reporting obligations** for actively exploited vulnerabilities and cybersecurity incidents apply **from 11 September 2026**, in line with CRA Article 14.
- **Full lifecycle vulnerability management requirements** apply to:
    - all **newly placed Poclain products** on the EU market from **11 December 2027**,
    - existing supported products for the duration of their declared support period.

This unified scope ensures that Poclain maintains a consistent, compliant, and coordinated approach to vulnerability handling across all relevant products and services.

# 3. Reporting a vulnerability

## 3.1 Preferred contact mechnism

Vulnerabilities should be reported to:

- **Email**: product.security@poclain.com
- **Subject**: Vulnerability Report – [Product/Component]
- **Web Form** (optional): [www...]

> All submissions are monitored by the Cybersecurity & Product Security Incident Response Team (PSIRT).

## 3.2 Required vulnerability report contents

To assist in efficient analysis, please include:

- Reporter name and contact information (*or remain anonymous*)
- Product name, version, and configuration details
- Detailed vulnerability description
- Steps to reproduce the issue
- Proof-of-concept (*if available*)
- Potential impact and suggested severity
- Relevant logs, captures, or screenshots
- Public references or prior disclosure history
- Desired disclosure expectations (*optional*)

> Incomplete reports will still be reviewed, although additional details may be requested.

## 3.3 How to submit a vulnerability

- Gather the relevant technical information
- Prepare the report (*see Section 3.2*)
- Submit via dedicated channels (*see Section 3.1*)
- Await acknowledgment and support investigation

## 4. Communication & coordination

Upon receiving a vulnerability report, Poclain commits to:

- Acknowledge receipt of the report in accordance with internal response SLAs within 48 hours
- Provide an initial assessment within 15 business days for all non-CRA cases
- Complete triage and classification within 24 hours for CRA-triggering cases, as required to meet the CRA Early Warning deadline (see Section 14.2).
- Keep the reporter informed of major investigation milestones
- Collaborate with the reporter throughout the remediation process
- Coordinate and negotiate a responsible disclosure timeline for non-CRA cases (90 calendar days)
- CRA notification deadlines are mandatory and not negotiable
- Inform impacted users when required by the CRA (Article 14), including in structured or machine-readable formats when applicable

The reporter is expected to:

- Maintain confidentiality during the remediation period and avoid premature disclosure
- Avoid publishing technical details, exploitation methods, or PoC before coordinated disclosure
- Provide additional information, clarification, or PoC if necessary to support analysis
- Engage constructively in achieving responsible and safe disclosure

> All reported vulnerabilities are handled in accordance the Poclain's internal Vulnerability Handling Process. This process includes triage, risk assessment, remediation decision, closure, and ensure compliance with applicable regulatory requirements.

## 5. Vulnerability eligibility

### 5.1 Accepted vulnerability types

Poclain primarily accepts reports related to:

- Embedded software and firmware vulnerabilities
- Bootloader and control software weaknesses
- Communication protocol vulnerabilities (CAN, LIN, Ethernet, wireless)
- Authentication, authorization, and access control issues
- Hardware security exposures (debug interfaces, memory access)
- Cloud service or API vulnerabilities
- Configuration weaknesses impacting safety or cybersecurity

### 5.2 OutofScope Items

Generally excluded:

- Social engineering
- Physical attacks requiring destructive product disassembly (unless security-relevant)
- Vulnerabilities in unsupported or end-of-life products
- Theoretical issues without practical or evidence of exploitability

## 6. Prioritization and handling overview

Vulnerabilities are prioritized based on:

- Safety, security, privacy, and operation continuity impact
- Exploitability and required access
- Asset criticality
- CVSS or equivalent scoring
- Required expertise or tools

Reports are accepted if:

- Sufficient information is provided
- The vulnerability is reproducible
- It affects a supported product

## 7. Disclosure & publication policy

### 7.1 Disclosure timeline

**Reminder:** CRA Article 14 requires manufacturers to notify **actively exploited vulnerabilities** and **severe incidents** within **24 h (Early Warning)**, **72 h (Full Notification)**, and **14 days / 1 month (Final Report)** through the **Single Reporting Platform (SRP)** to the **CSIRT coordinator** and **ENISA**.

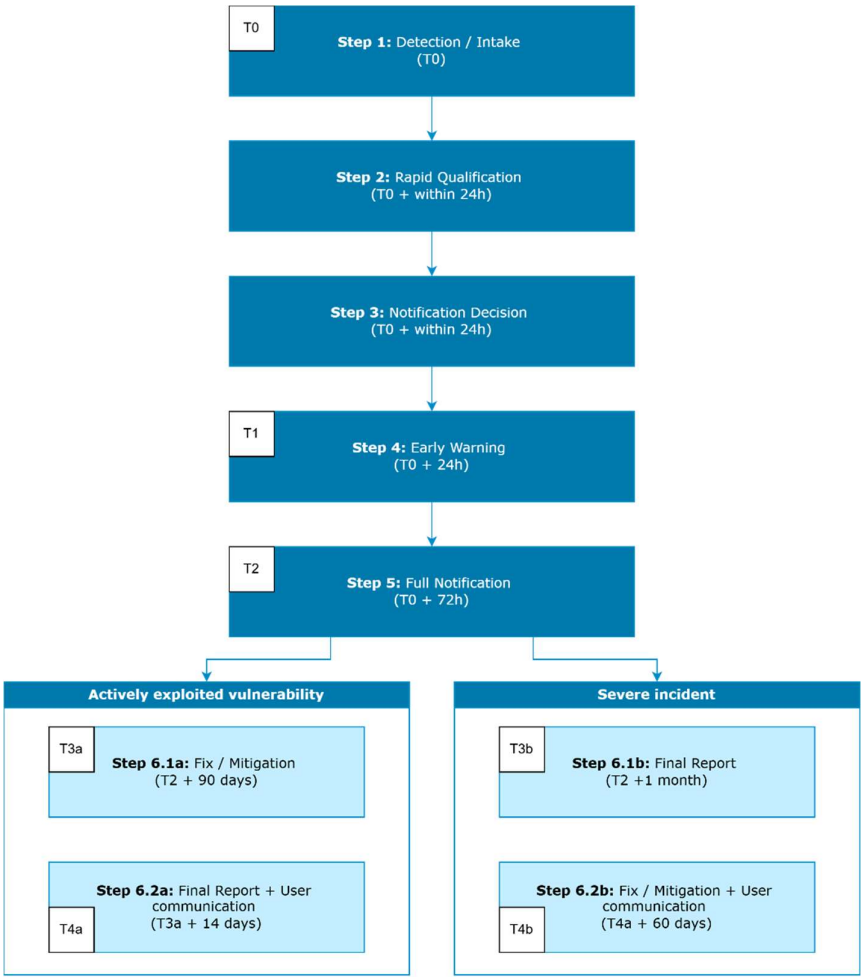


*Figure 1: Disclosure timeline*

### 7.1.1 Step 1: Detection / Intake (T0)

A vulnerability report is received through the official Poclain contact channels (email, web form).

Real-world triggers typically enter through **five main channels**:

1. A customer observing abnormal behaviour (crash, takeover, leak)
2. A security researcher reporting a vulnerability
3. A dependency alert (CVE / NVD / GitHub Advisory)
4. A CERT/CSIRT contacting the manufacturer
5. Internal logs or monitoring signals (e.g., detected exploitation attempts)

Upon receipt:

- The report is logged into the PSIRT system
- The reporter receives an acknowledgment according to internal SLAs
- Freeze of all useful elements: affected product/versions, logs, proof-of-exploit, vector, date/time, environment, reproduction artefacts
- Initial metadata (product, version, symptoms, PoC presence, reporter identity/anonymity) is captured

> **Note:** Intake alone does **not** trigger CRA notifications. CRA Article 14 is triggered **once Poclain becomes aware** of either an **actively exploited vulnerability** or a **severe incident** impacting the security of a product with digital elements (see Steps 2–3).

### 7.1.2 Step 2 : Rapid Qualification (T0 + within 24h)

This step focuses on the **triage, risk evaluation and classification** swiftly so that, if applicable, Poclain can issue the **Early Warning ≤ 24 hours from awareness**.

The objective is to answer **four simple questions**:

1. **Is it actually related to our product?**
   (CRA unit, affected versions, product context)
2. **What is the plausible impact?**
   (confidentiality, integrity, availability, loss of control)
3. **Is it actively exploited? (“a”)**
   (direct evidence, credible source, converging signals)
4. **Is this a severe incident? (“b”)**
   (important impact on the security of the PDE or users)

The goal of this step is to determine whether the case falls into:

- **“a” – Actively exploited vulnerability**
- **“b” – Severe incident impacting PDE security**
- **“c” – Other vulnerability (not CRA-triggering)**

The triage process includes:

1. **Reproducing or approximating the vulnerability impact** when possible within the time window.
2. **Determining whether exploitation is confirmed or reasonably suspected** (criteria for “a”).
3. **Determining if the event constitutes a severe security incident** as defined by CRA (criteria for “b”).
4. Evaluating potential safety, security, operational, and integrity impacts.
5. Deciding whether CRA statutory notifications (24h / 72h / 14 days or 1 month) apply.

> This rapid evaluation exists to ensure that Poclain can send an **Early Warning ≤ 24 h after becoming aware**, as required by CRA.

### 7.1.3 Step 3: Notification decision (T0 + within 24h)

The decision phase is critical: delaying or failing to decide is a compliance risk.

If there are **reasonable indications** of **active exploitation** (“**a**”) or a **severe incident** (“**b**”), proceed to **Early Warning (Step 4)**.
If the case is borderline:

- Document precisely why, **but still prepare the notification package** in advance (SRP template, facts, timeline, known impacts).
- This avoids losing precious time if the situation escalates.

> CRA requires manufacturers to notify **within 24 hours** once they become aware of an actively exploited vulnerability or a severe incident.

### 7.1.4 Step 4: Early warning (T1: T0 + 24h)

**Trigger:** classification “**a**” or “**b**” once Poclain becomes aware of the event.
**Channel:** SRP → CSIRT coordinator (+ simultaneous availability to ENISA).

**For actively exploited vulnerabilities (“a”):**

- Confirmation of active exploitation
- Member States where the product is available

**For severe incidents (“b”):**

- Confirmation of severe incident
- Whether malicious/unlawful acts are suspected
- Member States where the product is available

> **Deadline**: Without undue delay and in any event within **24 hours** of becoming aware.

### 7.1.5 Step 5: Full Notification (T2: T0 + 72h)

**Trigger:** same event as Step 4 (“a” or “b”).
**Channel:** SRP → CSIRT coordinator (+ simultaneous availability to ENISA).

Content requirements

**Vulnerability notification (“a”):**

- Product/component info
- General nature of the exploit and vulnerability
- Corrective/mitigating measures taken
- Mitigation steps users can implement
- Sensitivity classification

**Incident notification (“b”):**

- General information on the nature of the incident
- Initial assessment
- Measures taken
- Measures users can take
- Sensitivity classification

> **Deadline:** without undue delay and in any event within **72 hours of becoming aware** (if not already provided in the early warning).

### 7.1.6 Step 6: Treatment and final report

#### 7.1.6.1 Actively exploited vulnerability

**Step 6.1a:** Fix / Mitigation (**T3a**: T2 + 90 days)

From the **Full Notification step (T2)**, Poclain shall develop and deploy the required **corrective and/or mitigating** measures **within 90 days**.

In parallel, the CSIRT network may disseminate the notification to the relevant national CSIRTs and market surveillance authorities.

Exceptional delays in dissemination may occur on justified cybersecurity grounds.

**Step 6.2a:** Final Report + User communication (**T4a**: T3a + 14 days)

> Final report due no later than 14 days after a corrective or mitigating measure is available.

The final report shall include:

- Detailed description of the vulnerabilty (severity, impact)
- Information about malicious actors (if known)
- Details about security updates and/or mitigations provided

**User communication:**

At the same time, **Poclain shall communicate to impacted users** (and to **all users where appropriate**), potentially in **machine-readable** form, the vulnerability/incident information and the actions they must take.

#### 7.1.6.2 Severe incident

**Step 6.1b:** Final Report (**T3b**: T2 +1 month)

> Following the Full Notification step (T2), Poclain shall issue the Final Report within 1 month after the incident notification.

The final report shall include:

- Detailed description of the incident (severity, impact)
- Probable root cause or threat type
- Applied and ongoing mitigation measures

**Step 6.2b:** Fix / Mitigation + User communication (**T4b**: T4a + 60 days)

After the Final Report (T3b), Poclain **shall develop and deploy the corrective and/or mitigating measures within 60 days**.

In parallel, the CSIRT network may disseminate the notification to the relevant national CSIRTs and market surveillance authorities.

Exceptional delays in dissemination may occur on justified cybersecurity grounds.

**User communication:**

At the same time, **Poclain shall communicate to impacted users** (and to **all users where appropriate**), potentially in **machine-readable** form, the vulnerability/incident information and the actions they must take.

### 7.2 CVD-only cases (Non-exploited, Non-severe)

(CVD-Only Handling – See: Vulnerability Handling Process)

If no active exploitation and no severe incident:

- No CRA Article 14 notifications apply.
- Follow internal CVD lifecycle:
  - Detailed analysis
  - Prioritization
  - Remediation development & testing
  - Coordinated disclosure with reporter
  - Publication of a Security Advisory when mitigation is available

### 7.3 Publication policy

Final disclosure is **coordinated with the reporter** and may include:

- Security Advisory (SA)
- Mitigation instructions
- Firmware/software updates
- Public acknowledgment (if agreed)

Public disclosure occurs **only once mitigation is available**, or a **mutually agreed deadline** is reached. Premature public disclosure is avoided to protect operators and customers.

## 8. Legal considerations

Poclain commits to:

- Not initiating legal action against good-faith researchers
- Not restricting responsible research through DMCA-like constraints
- Cooperating with authorities where needed

Reporters must avoid:

- Damaging products or systems
- Accessing personal data
- Disrupting customer operations

Good-faith research is protected and encouraged.

## 9. Recognition of contributors

Poclain values contribution from the security community.
Reporters may request:

- Mention on Poclain's "*Hall of Thanks*"
- A certificate of contribution
- Full anonymity

**No financial rewards** are guaranteed unless part of a specific bounty program.

## 10. Associated documents

| ID | Document title | Reference |
|---|---|---|
| **Procedure** | | |
| | | |
| | | |
| | | |
| | | |
| **Policy** | | |
| | | |
| | | |
| | | |
| | | |
| **Rules** | | |
| | | |
| | | |
| | | |
| | | |
| **Template** | | |
| | | |
| | | |
| | | |
| | | |
| **Work Instruction** | | |
| | | |
| | | |
| | | |
| | | |
| **Appendix** | | |
| | | |
| | | |
| | | |
| | | |
| **Other** | | |
| | | |
| | | |
| | | |

## 11. Definitions

| Acronym | Definition |
|---|---|
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information |
| API | Application Programming Interface |
| CAN | Controller Area Network |
| CERT | Computer Emergency Response Team |
| CRA | Cyber Resilience Act |
| CSIRT | Computer Security Incident Response Team |
| CVD | Coordinated Vulnerability Disclosure |
| CVE | Common Vulnerabilities and Exposures |
| CVSS | Common Vulnerability Scoring System |
| DMCA | Digital Millennium Copyright Act |
| ENISA | European Union Agency for Cybersecurity |
| LIN | Local Interconnect Network |
| NVC | Non-Vulnerability Case |
| PDEs | Products with Digital Elements |
| PoC | Proof of Concept |
| PSIRT | Product Security Incident Response Team |
| SA | Security Advisory |
| SLA | Service Level Agreement |
| SRP | Single Reporting Platform |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## 12. Revision history

| Version | Date | Description | Author |
|---|---|---|---|
| A | 2026.03.11 | Initial policy release | A. Laumonnier |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |