

▼ PURPOSE OF DOCUMENT

This document defines the Coordinated Vulnerability Disclosure (CVD) Policy of Ecorobotix. It sets out the terms of engagement between Ecorobotix and any individual or organization - hereafter referred to as the reporter - who discovers a potential vulnerability in an Ecorobotix product or service.

Ecorobotix is committed to working collaboratively with the security research community to identify and address vulnerabilities responsibly. This policy is designed to encourage good-faith disclosure, protect reporters who act within its boundaries, and ensure that vulnerabilities are resolved in a timely and transparent manner.

▼ SCOPE OF APPLICATION

This policy applies to all Ecorobotix software, firmware, hardware products, and associated cloud services placed on the market, including but not limited to:

- Embedded operating systems, firmware and application running on Ecorobotix machines
- Cloud services and APIs used for machine management and telemetry
- Mobile or desktop applications provided by Ecorobotix
- Third-party components integrated into Ecorobotix products

This policy does not cover vulnerabilities in third-party products or services not distributed by Ecorobotix. For such findings, please report directly to the relevant vendor

TABLE OF CONTENTS

▼	PURPOSE OF DOCUMENT	1
▼	SCOPE OF APPLICATION	1
1	HOW TO REPORT A VULNERABILITY	3
2	WHAT YOU CAN EXPECT FROM ECOROBOTIX	3
3	SAFE HARBOUR - REPORTER PROTECTIONS	3
4	COORDINATED DISCLOSURE	4
5	PUBLIC DISCLOSURE & SECURITY ADVISORIES	4
6	OUT OF SCOPE	4
▼	RELATED TEMPLATES, INSTRUCTIONS & RULES	5
▼	GLOSSARY	5

1 HOW TO REPORT A VULNERABILITY

If you believe you have discovered a vulnerability in an Ecorobotix product or service, we encourage you to report it to us as soon as possible. Responsible disclosure gives us the opportunity to investigate and remediate the issue before it can be exploited.

Please submit your report to the following security contact:

Channel	Details
Email	csirt@ecorobotix.com
Language	English or French

To help us triage the report efficiently, please include the following information where possible:

- A clear description of the vulnerability and the affected product or component
- The version or configuration in which the vulnerability was observed
- Steps to reproduce the issue or a proof of concept
- The potential impact you believe the vulnerability could have
- Your contact details for follow-up (optional but appreciated)

2 WHAT YOU CAN EXPECT FROM ECOROBOTIX

Ecorobotix is committed to handling all vulnerability reports professionally and transparently. Upon receiving your report, you can expect the following:

Commitment	Timeframe
Acknowledgement of your report	Within 5 business days
Initial assessment and confirmation of the finding	Within 15 business days
Regular status updates throughout the resolution process	Every 30 days or upon significant progress
Notification when the vulnerability has been resolved	Upon patch release
Publication of fixed vulnerability information (CVE, versions)	Upon patch release
Publication of machine-readable CSAF 2.0 security advisory	Upon patch release
Public acknowledgement of your contribution (if desired)	Upon public disclosure

3 SAFE HARBOUR - REPORTER PROTECTIONS

Ecorobotix values the contribution of security researchers and is committed to protecting reporters who act in good faith. If you comply with this policy, Ecorobotix commits to:

- Not initiating or recommending legal action against you in relation to your research
- Not treating your report as a hostile act
- Working with you in good faith to understand and resolve the issue
- Keeping your identity confidential if you request anonymity

Safe harbour applies provided that the reporter:

- Does not access, modify, or delete data beyond what is strictly necessary to demonstrate the vulnerability
- Does not exploit the vulnerability for any purpose other than demonstrating its existence

- Does not disclose the vulnerability publicly before Ecorobotix has had a reasonable opportunity to remediate it
- Does not conduct testing that could disrupt Ecorobotix services or harm third parties
- Acts in good faith and without malicious intent

4 COORDINATED DISCLOSURE

Ecorobotix follows a coordinated disclosure approach. This means we ask reporters to refrain from publicly disclosing vulnerability details until we have had a reasonable opportunity to investigate and release a fix.

Our target resolution timeline is defined by the severity of the vulnerability:

Severity	Target Patch/Mitigation Deadline
Critical (CVSS 9.0 – 10.0)	As soon as possible (7 days)
High (CVSS 7.0 – 8.9)	As soon as possible (30 days)
Medium (CVSS 4.0 – 6.9)	Best effort - prioritized after Critical/High (60 days)
Low (CVSS 0.1 – 3.9)	Next planned release - no fixed deadline

If we are unable to meet a deadline, we will notify the reporter and agree on an extension. We will never ask a reporter to delay disclosure indefinitely.

5 PUBLIC DISCLOSURE & SECURITY ADVISORIES

Once a vulnerability has been remediated, Ecorobotix commits to publishing the following information publicly:

- The CVE identifier (if assigned) or a clear description of the vulnerability
- The affected product names and versions
- The corrective measures applied
- The patch or release containing the fix

In accordance with CRA Annex I Part II §5, Ecorobotix will publish machine-readable security advisories in CSAF 2.0 format for significant vulnerabilities.

6 OUT OF SCOPE

The following types of findings are out of scope for this policy and will not be actioned as security vulnerabilities:

- Vulnerabilities in third-party products or services not distributed by Ecorobotix
- Social engineering or phishing attacks targeting Ecorobotix employees
- Denial of service attacks or volumetric testing
- Physical attacks on Ecorobotix hardware or facilities
- Reports generated by automated scanning tools without manual validation

▼ RELATED TEMPLATES, INSTRUCTIONS & RULES

- [Cyber Resilience Act\(CRA\)](#)
- [FIRST CVD Guide](#)

▼ GLOSSARY

Terms and acronyms (in alphabetical order)	
CVD	Coordinated Vulnerability Disclosure - a process for responsibly reporting and resolving security vulnerabilities
CRA	EU Cyber Resilience Act
CVSS	Common Vulnerability Scoring System - framework for rating vulnerability severity
CSIRT	Computer Security Incident Response Team
PGP	Pretty Good Privacy - encryption standard for secure email communication
Safe harbour	Legal and ethical protection granted to good-faith security researchers
CSAF	Common Security Advisory Framework - standard JSON format for machine-readable security advisories (v2.0 required by CRA Annex I Part II §5)
CVE	Common Vulnerabilities and Exposures - standard identifier for publicly known vulnerabilities