LEROY AUTOMATION's Coordinated Disclosure Policy

Introduction

LEROY AUTOMATION welcomes feedback from security researchers and the public to improve the security of our products. If you believe you have discovered a vulnerability, privacy issue, data exposure, or any other security issue affecting any of our assets, we want to hear from you.
This policy, in accordance with Regulation **(EU) 2024/2847: Cyber Resilience Act (CRA),** outlines the steps to take to report vulnerabilities to us, what we expect from you, and what you can expect from us.

Systems in Scope

This policy applies to any product manufactured by LEROY AUTOMATION.

Out-of-Scope Assets

- Assets or other equipment that are not manufactured by LEROY AUTOMATION.
- Vulnerabilities discovered or suspected in out-of-scope systems SHALL be reported to the relevant provider or competent authority.

Our commitments

When you work with us in accordance with this policy, you can expect LEROY AUTOMATION to:

- respond promptly to your report and work with you to understand and validate it
- work to keep you informed of the progress of the vulnerability
- strives to remediate discovered vulnerabilities in a timely manner, considering its operational constraints
- apply the Safe Harbor provisions to vulnerability research conducted under this policy
- handle the information provided securely and apply industry standards to ensure confidentiality

Our expectations

As part of a good faith participation in our vulnerability disclosure program, we ask that you:

- comply with the rules, including this Policy and any other relevant agreements. In the event of any inconsistency between this Policy and other applicable terms, the provisions of this Policy shall prevail
- Report any discovered vulnerability promptly and no later than 72 hours after it is discovered
- Avoid infringing on the privacy of others, disrupting our systems or those of our customers, destroying data, or degrading the user experience
- Use only official channels to communicate with us about vulnerabilities
- allow us a reasonable period of at least 30 days from the initial report, to resolve the issue before any public disclosure
- conduct testing only on systems that are in scope and respect out-of-scope systems and activities
- If a vulnerability gives access to user data, including personal data, health data, credit card data, or proprietary information, stop testing and report immediately.
- Interact only with test accounts that you own or for which you have explicit permission from the owner
- do not engage in any form of extortion

Official Channel

Please report any safety issues to PSIRT@leroy-agon.com, providing all relevant information. The more detailed the information provided, the easier it will be for us to qualify, triage, and correct the issue.

Safe Harbor

When you conduct vulnerability scans in accordance with this policy, we consider that research to be:

- permitted under applicable anti-piracy laws; we will not take or support any legal action against you for an accidental and bona fide breach of this Policy
- permitted under applicable laws on circumvention of technological measures; we will not take any action against you for circumvention of technological controls
- exempt from the restrictions in our Terms of Service or Acceptable Use Policy that would prevent the conduct of security research, and we waive these restrictions to a limited extent.

You remain responsible for always complying with all applicable laws.
If legal action is taken by a third party against you while you have complied with this policy, we will take steps to make it known that your actions have been carried out in accordance with this policy.
If you have any concerns or are unsure if your security searches are in line with this policy, please submit a report through one of our official channels before proceeding further.
The Safe Harbor provisions apply only to legal claims within the control of the organization participating in this policy. It is not binding on independent third parties.

LEROY AUTOMATION Disclosure policy

LEROY AUTOMATION acts in good faith with respect to Reporters who discover, test and report vulnerabilities or indicators of vulnerability in accordance with these guidelines.
Note: In the remainder of the document, the terms MAY, SHOULD, MUST and SHALL are used according to RFC 2119 to eliminate ambiguity.

General provisions

- LEROY AUTOMATION MAY modify the provisions of this Policy or terminate it at any time.
- LEROY AUTOMATION SHALL use the information reported under this program solely for defensive purposes, to mitigate or remediate vulnerabilities affecting its products or applications.

Case Handling

- LEROY AUTOMATION MAY, at its discretion, refuse to coordinate or publish a vulnerability report. This decision is generally based on the scope and severity of the vulnerability as well as our ability to add value to the coordination and disclosure process.
- LEROY AUTOMATION SHALL review each reported vulnerability and make reasonable efforts to ensure that appropriate measures are taken to mitigate the risk and remediate the reported vulnerabilities.
- LEROY AUTOMATION SHALL determine an appropriate timeframe for the development and deployment of mitigation measures for reported vulnerabilities in the systems under its control.

Coordination with Reporters

- LEROY AUTOMATION SHALL acknowledge receipt of vulnerability reports by e-mail within 72 business hours.
- LEROY AUTOMATION MAY contact the Reporter to request additional information.
- LEROY AUTOMATION SHALL inform the Reporter of the results of the vulnerability validation, where appropriate, and provide status information on the progress of the remediation implementation.
- LEROY AUTOMATION SHALL mention the Reporter in any published vulnerability notice, unless otherwise requested by LEROY AUTOMATION.
- LEROY AUTOMATION SHALL use the reporter's personal data solely to carry out activities related to the reported vulnerabilities. Such data will not be disclosed to third parties without the reporter's consent, unless required by law.
- LEROY AUTOMATION SHALL protect reporter's personal data in accordance with the GDPR.
- LEROY AUTOMATION MAY adjust its publication schedule to accommodate the Reporter's constraints, provided that the schedule remains compatible with this policy. However, such an adjustment constitutes a postponement and not an acceleration of the publication schedule. This may include postponing publication to coincide with a presentation at a conference.
- LEROY AUTOMATION SHALL NOT require Reporters to establish a customer relationship, enter into a non-disclosure agreement (NDA), or incur any other contractual or financial obligation as a condition of receiving or coordinating a vulnerability report.

Coordination with suppliers

- If LEROY AUTOMATION determines that the reported vulnerability results from a vulnerability affecting a generally available product or service (COTS), LEROY AUTOMATION may report it to the relevant vendors, service providers, or third-party vulnerability coordination services to enable remediation of the product or service.

- LEROY AUTOMATION SHOULD notify vendors of reported vulnerabilities prior to any public disclosure.
- LEROY AUTOMATION SHALL NOT disclose information provided confidentially by a supplier.
- When acting as a Reporter to other organizations, including vendors or coordinators, LEROY AUTOMATION SHALL comply with the expectations applicable to Reporters set forth in this policy.

Coordination with other parties

- LEROY AUTOMATION MAY engage a third-party coordination service, such as ANSSI or ENISA, to assist in the resolution of any disagreement that cannot be resolved between the Reporter and LEROY AUTOMATION.
- LEROY AUTOMATION MAY, at its discretion, share information about a reported vulnerability to anyone who may be involved in its resolution and with whom it has a trusted relationship, including vendors, service providers, community experts, sponsors, and national critical infrastructure sites, if it believes that such sites are at risk.

Public Disclosure

- LEROY AUTOMATION SHALL determine the nature and timing of the public disclosure of the vulnerability.
- LEROY AUTOMATION MAY publicly disclose reported vulnerabilities 15 days after the initial report, regardless of the existence or availability of fixes or workarounds offered by the relevant vendors, in the dedicated section of LEROY AUTOMATION's website: Cybersecurity at LEROY AUTOMATION
- LEROY AUTOMATION MAY disclose vulnerabilities before or after this 15-day period due to exceptional circumstances, including active exploitation, threats of a particularly serious or minor nature, or situations requiring the modification of an established standard.
- LEROY AUTOMATION MAY consult with the reporter and relevant suppliers to determine the appropriate timing and terms of public disclosure.

Reporter Reporting Policy

Notifiers SHALL comply with the following guidelines.

General provisions

- Reporters SHALL comply with all applicable laws in connection with their security research activities or any other participation in this vulnerability disclosure program.
- Reporters SHOULD make good faith efforts to inform and collaborate directly with affected providers or service providers prior to any public disclosure of a vulnerability report.

Scope of authorized testing

- Reporters MAY test LEROY AUTOMATION's products for vulnerabilities solely for the purpose of providing LEROY AUTOMATION with information about the vulnerability.
- Reporters SHALL NOT conduct testing on a product while it is in use by a legitimate user.
- Reporters SHALL make every effort to avoid privacy violations, degradation of user experience, and destruction or manipulation of data.
- Reporters SHALL stop testing as soon as they have established the existence of a vulnerability or encountered sensitive data. Sensitive data includes personal data, financial information, proprietary information, and trade secrets.
- Reporters SHALL NOT exploit a vulnerability beyond the minimum level of testing necessary to demonstrate its existence or identify an associated indicator.
- Reporters SHALL NOT intentionally access the content of communications, data or information passing through LEROY AUTOMATION's information systems or stored there.
- Reporters SHALL NOT intentionally compromise the privacy or security of LEROY AUTOMATION's personnel, its customers, the public, or legitimate third parties.
- Reporters SHALL NOT exploit discovered vulnerabilities to pivot to other systems.
- Reporters SHALL NOT intentionally infringe on the intellectual property or other commercial or financial interests of users of LEROY AUTOMATION's products.
- Reporters SHALL NOT cause a legitimate service to become unavailable during their testing.
- Reporters SHALL NOT carry out any social engineering operation, in any form whatsoever, against LEROY AUTOMATION's staff or service providers.

Reporters SHOULD contact LEROY AUTOMATION at PSIRT@leroy-agon.com if they are unsure at any time whether they can continue their testing.

Coordination with LEROY AUTOMATION

- Reporters SHALL submit their vulnerability reports to LEROY AUTOMATION via the official PSIRT@leroy-agon.com channel.
- Reporters SHOULD include sufficient descriptive detail to enable LEROY AUTOMATION and, where appropriate, the relevant suppliers to accurately replicate the vulnerable behavior.
- Reporters SHALL preserve the confidentiality of any information related to vulnerabilities. This requirement does not preclude the simultaneous coordination of the report with other relevant parties, including suppliers, service providers or coordinators.
- Reporters MAY request that their contact details not be disclosed to the relevant suppliers.
- Reporters MAY request not to be named in the acknowledgments associated with LEROY AUTOMATION's public disclosures.
- Reporters SHALL NOT require LEROY AUTOMATION enter into a contractual or financial obligation as a condition of submitting a vulnerability report.
- Reporters SHALL NOT demand payment for reporting a vulnerability outside of an explicit bug bounty program.

Coordination with suppliers

When a Reporter discovers, in a LEROY AUTOMATION product, a vulnerability resulting from a vulnerability affecting a generally available product or service, it MAY report it to the relevant vendors, service providers, or a third-party vulnerability coordination service, without disclosing any sensitive information regarding the LEROY AUTOMATION product, in order to enable the remediation of the product or service.

Coordination with other parties

Reporters SHOULD NOT disclose any details of any extent regarding a vulnerability affecting a LEROY AUTOMATION product, or any indicators of vulnerability, to any party that was not already aware of it at the time the report is forwarded to LEROY AUTOMATION.

Public Disclosure

- Reporters MAY publicly disclose the prior existence of vulnerabilities already remediated by LEROY AUTOMATION, including potential vulnerability information, indicators of vulnerability, or the nature, but not the content, of the information to which the vulnerability has given access.
- Reporters who choose public disclosure SHALL proceed in coordination with LEROY AUTOMATION.
- Reporters SHALL NOT disclose to any party that was not already aware of it when reporting to LEROY AUTOMATION the proprietary data discovered incidentally during testing or the content of the information made accessible by the vulnerability.

Appendix 1: Disclosure Sheet

Contact:

You should send the discovered information exclusively to the following email address: PSIRT@leroy-agon.com.
Whenever possible, we encourage you to use secure PGP communication using the following information:

PGP Key ID: 1668FD92
PGP Key Type: RSA-4096 Key
PGP Key Fingerprint: A7B9 E8AA F0AA AF13 C13D 3524 3FBC 9FC1 1668 FD92

Please provide at least the following relevant information:

Last Name: First name:	
Email address: Phone Number: Address:	
Vulnerability description:	
Vulnerability Type:	
Configuration Details:	
Operations performed (logs):	
Tools used:	
Test dates and times:	
Any other relevant information:	