

Leroy-Automation Vulnerability Disclosure Policy

Introduction

Leroy-Automation welcomes feedback from security researchers and the public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you.

This policy outlines steps for reporting vulnerabilities to us, what we expect, what you can expect from us.

Systems in Scope

This policy applies to any Leroy-Automation's product.

Out of Scope

Assets or other equipment not manufactured by Leroy-Automation.

Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

Our Commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report
- Strive to keep you informed about the progress of a vulnerability as it is processed
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints
- Extend Safe Harbor for your vulnerability research that is related to this policy
- Treat the information provided securely and apply industry standards to ensure confidentiality.

Our Expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail
- Report any vulnerability you've discovered promptly and **at the latest 72h after the discovery**
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience
- Use only the Official Channels to discuss vulnerability information with us
- Provide us a reasonable amount of time (**at least 30 days from the initial report**) to resolve the issue before you disclose it publicly
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally

Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information

- You should only interact with test accounts you own or with explicit permission from the account holder
- Do not engage in extortion

Official Channel

Please report security issues via PSIRT@leroy-agon.com , providing all relevant information. The more details you provide, the easier it will be for us to process triage and fix the issue.

Safe Harbor

When conducting vulnerability research, according to this policy, we consider this research conducted under this policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls
- Exempt from restrictions in our Terms of Service and/or Acceptable Usage Policy that would interfere with conducting security research, and we waive those restrictions on a limited basis

You are expected, as always, to **comply with all applicable laws**. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

Note that the Safe Harbor applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.

LEROY-Automation Policy Statements

LEROY-AUTOMATION will deal in good faith with Reporters who discover, test, and report vulnerabilities or indicators of vulnerabilities in accordance with these guidelines.

Note: in the following document, words like MAY, SHOULD, MUST, and SHALL are used according to [RFC 2119](#) to eliminate ambiguity.

General

- LEROY-AUTOMATION MAY modify the terms of this policy or terminate the policy at any time.
- LEROY-AUTOMATION SHALL use information reported to this program for defensive purposes only; to mitigate or remediate vulnerabilities in our products or applications.

Case handling

- LEROY-AUTOMATION MAY, at our discretion, decline to coordinate or publish a vulnerability report. This decision is generally based on the scope and severity of the vulnerability and our ability to add value to the coordination and disclosure process.
- LEROY-AUTOMATION SHALL investigate every reported vulnerability and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.
- LEROY-AUTOMATION SHALL determine an appropriate timeframe for mitigation development and deployment for vulnerabilities reported in systems it controls.

Coordination with reporters

- LEROY-AUTOMATION SHALL acknowledge receipt of vulnerability reports via email within 72 business hours.
- LEROY-AUTOMATION MAY contact the Reporter for further information.
- LEROY-AUTOMATION SHALL inform the Reporter of the results of vulnerability validation, as appropriate, and accordingly provide status updates as remediation of the vulnerability is underway.
- LEROY-AUTOMATION SHALL include credit to the reporter in any published vulnerability report unless otherwise requested by the reporter.
- LEROY-AUTOMATION SHALL use reporter's personal data only to carry out actions related to reported security vulnerabilities. It will not be disclosed to third parties without the consent of the reporter, unless required by law.
- LEROY-AUTOMATION MAY adjust its publication timeframe to accommodate reporter constraints if that timing is otherwise compatible with this policy. Nevertheless, such an adjustment would represent a delay rather than an acceleration of the publication schedule. Examples include delaying publication to coincide with conference presentations.
- LEROY-AUTOMATION SHALL NOT require reporters to enter into a customer relationship, non-disclosure agreement (**NDA**) or any other contractual or financial obligation as a condition of receiving or coordinating vulnerability reports.

Coordination with vendors

- If LEROY-AUTOMATION determines the reported vulnerability is consequent to a vulnerability in a generally available product or service, LEROY-AUTOMATION MAY report the vulnerability to the affected vendor(s), service provider(s), or third-party vulnerability coordination service(s) in order to enable the product or service to be fixed.

- LEROY-AUTOMATION SHALL make a good faith effort to inform vendors of reported vulnerabilities prior to public disclosure.
- LEROY-AUTOMATION SHALL NOT reveal information provided in confidence by any vendor.
- LEROY-AUTOMATION SHALL act in accordance with the expectations of Reporters set forth in this policy when acting as a Reporter to other organizations (vendors, coordinators, etc.).

Coordination with others

- LEROY-AUTOMATION MAY engage the services of a third-party coordination service (e.g., ANSSI, ENISA) to assist in resolving any conflicts that cannot be resolved between the Reporter and LEROY-AUTOMATION.
- LEROY-AUTOMATION MAY, at our discretion, provide reported vulnerability information to anyone who can contribute to the solution and with whom we have a trusted relationship, including vendors, service providers, community experts, sponsors, and sites that are part of a national critical infrastructure, if we believe those sites to be at risk.

Public disclosure

- LEROY-AUTOMATION SHALL determine the type and schedule of our public disclosure of the vulnerability.
- LEROY-AUTOMATION MAY disclose reported vulnerabilities to the public 15 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors on Leroy-Automation website dedicated section: <https://www.leroy-automation.com/en/cybersecurity-leroy-automation/>
- LEROY-AUTOMATION MAY disclose vulnerabilities to the public earlier or later than 15 days due to extenuating circumstances, including but not limited to active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard.
- LEROY-AUTOMATION MAY consult with the Reporter and any affected vendor(s) to determine the appropriate public disclosure timing and details.

Reporters Policy Statements

Reporters MUST adhere to the following guidelines.

General

- Reporters MUST comply with all applicable laws in connection with security research activities or other participation in this vulnerability disclosure program.
- Reporters SHOULD make a good faith effort to notify and work directly with the affected vendor(s) or service providers prior to publicly disclosing vulnerability reports.

Scope of Authorized Testing

- Reporters MAY test LEROY-AUTOMATION's products to detect a vulnerability for the sole purpose of providing LEROY-AUTOMATION information about that vulnerability.
- Reporters MUST make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Reporters MUST stop testing once that testing has established that a vulnerability exists, or sensitive data has been encountered. Sensitive data includes personally identifiable information, financial information, proprietary information or trade secrets.
- Reporters MUST NOT exploit any vulnerability beyond the minimal amount of testing required to prove that the vulnerability exists or to identify an indicator related to that vulnerability.
- Reporters MUST NOT intentionally access the content of any communications, data, or information transiting or stored on LEROY-AUTOMATION's information systems.
- Reporters MUST NOT intentionally compromise the privacy or safety of LEROY-AUTOMATION's personnel, customers, the general public, or any legitimate third parties.
- Reporters MUST NOT exploit any vulnerabilities found to pivot to other systems.
- Reporters MUST NOT intentionally compromise the intellectual property or other commercial or financial interests of any LEROY-AUTOMATION's product user.
- Reporters MUST NOT cause a denial of any legitimate services during their testing.
- Reporters MUST NOT conduct social engineering in any form of LEROY-AUTOMATION personnel or contractors.
- Reporters SHOULD contact LEROY-AUTOMATION at PSIRT@leroy-agon.com if at any point you are uncertain of whether to proceed with testing.

Coordination with LEROY-AUTOMATION

- Reporters SHOULD submit vulnerability reports to LEROY-AUTOMATION via PSIRT@leroy-agon.com.
- Reporters SHOULD include sufficient descriptive details to permit LEROY-AUTOMATION and/or the affected vendor(s) to accurately reproduce the vulnerable behavior.
- Reporters SHOULD NOT report unanalyzed crash dumps or fuzzer output unless accompanied by a sufficiently detailed explanation of how they represent a security vulnerability.
- Reporters MUST keep confidential any information about vulnerabilities. Notwithstanding, this expectation does not preclude Reporters from simultaneously coordinating the vulnerability report with other affected parties (vendors, service providers, coordinators, etc.)
- Reporters MAY request that their contact information be withheld from all affected vendor(s).
- Reporters MAY request not to be named in the acknowledgements of LEROY-AUTOMATION's public disclosures.

- Reporters **MUST NOT** require LEROY-AUTOMATION to enter into contractual or financial obligation as a condition of providing vulnerability reports.
- Reporters **MUST NOT** demand compensation in return for reporting vulnerability information reported outside of an explicit bug bounty program.

Coordination with vendors

- In the event that the Reporter finds a vulnerability in a LEROY-AUTOMATION's product consequent to a vulnerability in a generally available product or service, the Reporter **MAY** report the vulnerability to the affected vendor(s), service provider(s), or third-party vulnerability coordination service(s) without disclosing any sensible information about LEROY-AUTOMATION's product in order to enable the product or service to be fixed.

Coordination with others

- Reporters **SHOULD NOT** disclose any details of any extent LEROY-AUTOMATION's product vulnerability, or any indicators of vulnerability to any party not already aware at the time the report is submitted to LEROY-AUTOMATION.

Public disclosure

- Reporters **MAY** disclose to the public the prior existence of vulnerabilities already fixed by LEROY-AUTOMATION, including potential details of the vulnerability, indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability.
- Reporters choosing to disclose to the public **SHALL** do so in consultation with LEROY-AUTOMATION.
- Reporters **MUST NOT** disclose any incidental proprietary data revealed during testing or the content of information rendered available by the vulnerability to any party not already aware at the time the report is submitted to LEROY-AUTOMATION.