Politique de Divulgation Coordonnée de LEROY AUTOMATION

Introduction

LEROY AUTOMATION accueille favorablement les retours des chercheurs en sécurité et du public afin d'améliorer la sécurité de ses produits. Si vous pensez avoir découvert une vulnérabilité, un problème de confidentialité, une exposition de données ou tout autre problème de sécurité affectant l'un de nos actifs, nous souhaitons en être informés.
La présente politique, en accord avec le règlement **(EU) 2024/2847: Cyber Resilience Act (CRA),** décrit les étapes à suivre pour nous signaler des vulnérabilités, ce que nous attendons de vous et ce que vous pouvez attendre de nous.

Systèmes inclus dans le périmètre

La présente politique s'applique à tout produit fabriqué par LEROY AUTOMATION.

Éléments hors périmètre

- Les actifs ou autres équipements qui ne sont pas fabriqués par LEROY AUTOMATION.
- Les vulnérabilités découvertes ou suspectées dans des systèmes hors périmètre doivent être signalées au fournisseur concerné ou à l'autorité compétente.

Nos engagements

Lorsque vous collaborez avec nous conformément à la présente politique, vous pouvez attendre de LEROY AUTOMATION qu'elle :

- réponde rapidement à votre signalement et collabore avec vous afin de le comprendre et de le valider
- s'efforce de vous tenir informé de l'avancement du traitement de la vulnérabilité
- s'efforce de remédier aux vulnérabilités découvertes dans des délais appropriés, compte tenu de ses contraintes opérationnelles
- applique la clause de protection (« Safe Harbor ») aux recherches de vulnérabilités relevant de la présente politique
- traite les informations fournies de manière sécurisée et applique les normes du secteur afin d'en garantir la confidentialité

Nos attentes

Dans le cadre d'une participation de bonne foi à notre programme de divulgation des vulnérabilités, nous vous demandons de :

- respecter les règles, notamment la présente politique et tout autre accord pertinent. En cas d'incohérence entre la présente politique et d'autres conditions applicables, les dispositions de la présente politique prévalent
- signaler rapidement toute vulnérabilité découverte et, au plus tard, dans les 72 heures suivant sa découverte
- éviter de porter atteinte à la vie privée d'autrui, de perturber nos systèmes ou ceux de nos clients, de détruire des données ou de dégrader l'expérience utilisateur
- utiliser uniquement les canaux officiels pour échanger avec nous au sujet des vulnérabilités
- nous accorder un délai raisonnable, d'au moins 30 jours à compter du signalement initial, pour résoudre le problème avant toute divulgation publique

- effectuer les tests uniquement sur les systèmes inclus dans le périmètre et respecter les systèmes et activités hors périmètre
- si une vulnérabilité donne un accès à des données utilisateur, notamment des données à caractère personnel, des données de santé, des données de carte bancaire ou des informations propriétaires, interrompre les tests et transmettre immédiatement un signalement.
- interagir uniquement avec des comptes de test dont vous êtes propriétaire ou pour lesquels vous disposez de l'autorisation explicite du titulaire
- ne vous livrer à aucune forme d'extorsion

Canal officiel

Veuillez signaler les problèmes de sécurité à l'adresse PSIRT@leroy-agon.com, en fournissant toutes les informations pertinentes. Plus les informations transmises seront détaillées, plus il nous sera facile d'effectuer la qualification, le triage et la correction du problème.

Clause de protection (« Safe Harbor »)

Lorsque vous menez des recherches de vulnérabilités conformément à la présente politique, nous considérons que ces recherches sont :

- autorisées au regard des lois applicables en matière de lutte contre le piratage informatique ; nous n'engagerons ni ne soutiendrons d'action en justice à votre encontre en cas de violation accidentelle et de bonne foi de la présente politique
- autorisées au regard des lois applicables en matière de contournement des mesures techniques ; nous n'intenterons aucune action à votre encontre du fait du contournement de contrôles technologiques
- exemptées des restrictions prévues dans nos conditions de service ou notre politique d'utilisation acceptable lorsqu'elles empêcheraient la conduite de recherches de sécurité, nous renonçons à ces restrictions de manière limitée.

Vous êtes tenu, en toutes circonstances, de respecter l'ensemble des lois applicables.
Si une action en justice est engagée par un tiers à votre encontre alors que vous avez respecté la présente politique, nous prendrons des mesures afin de faire savoir que vos actions ont été menées conformément à celle-ci.
Si vous avez des préoccupations ou ne savez pas si vos recherches de sécurité sont conformes à la présente politique, veuillez soumettre un signalement par l'un de nos canaux officiels avant d'aller plus loin.
La clause de protection s'applique uniquement aux réclamations juridiques relevant du contrôle de l'organisation participant à la présente politique. Elle ne lie pas les tiers indépendants.

Politique de déclaration de LEROY AUTOMATION

LEROY AUTOMATION agit de bonne foi à l'égard des déclarants qui découvrent, testent et signalent des vulnérabilités ou des indicateurs de vulnérabilité conformément aux présentes lignes directrices.
Note : dans la suite du document, les termes PEUT (MAY), DEVRAIT (SHOULD) et DEVRA (SHALL) sont employés conformément à la RFC 2119 afin d'éliminer toute ambiguïté.

Dispositions générales

- LEROY AUTOMATION PEUT modifier les dispositions de la présente politique ou mettre fin à celle-ci à tout moment.
- LEROY AUTOMATION DEVRA utiliser les informations signalées dans le cadre de ce programme uniquement à des fins défensives, afin d'atténuer ou de corriger les vulnérabilités affectant ses produits ou applications.

Traitement des cas

- LEROY AUTOMATION PEUT, à sa discrétion, refuser de coordonner ou de publier un signalement de vulnérabilité. Cette décision repose généralement sur le périmètre et la gravité de la vulnérabilité ainsi que sur notre capacité à apporter une valeur ajoutée au processus de coordination et de divulgation.
- LEROY AUTOMATION DEVRA examiner chaque vulnérabilité signalée et s'efforcer de veiller à ce que les mesures appropriées soient prises pour atténuer le risque et corriger les vulnérabilités signalées.
- LEROY AUTOMATION DEVRA déterminer un délai approprié pour le développement et le déploiement des mesures d'atténuation concernant les vulnérabilités signalées dans les systèmes qu'elle contrôle.

Coordination avec les déclarants

- LEROY AUTOMATION DEVRA accuser réception des signalements de vulnérabilité par courrier électronique dans un délai de 72 heures ouvrées.
- LEROY AUTOMATION PEUT contacter le déclarant afin d'obtenir des informations complémentaires.
- LEROY AUTOMATION DEVRA informer le déclarant des résultats de la validation de la vulnérabilité, lorsque cela est approprié, et lui fournir des informations d'avancement de la mise en œuvre de la correction.
- LEROY AUTOMATION DEVRA mentionner le déclarant dans tout avis de vulnérabilité publié, sauf demande contraire de sa part.
- LEROY AUTOMATION DEVRA utiliser les données personnelles du déclarant uniquement pour mener les actions liées aux vulnérabilités signalées. Elles ne seront pas communiquées à des tiers sans le consentement du déclarant, sauf obligation légale.
- LEROY AUTOMATION DEVRA protéger les données personnelles du déclarant au titre du RGPD.
- LEROY AUTOMATION PEUT ajuster son calendrier de publication afin de tenir compte des contraintes du déclarant, si ce calendrier reste compatible avec la présente politique. Un tel ajustement constitue toutefois un report et non une accélération du calendrier de publication. Il peut notamment s'agir de reporter la publication pour la faire coïncider avec une présentation lors d'une conférence.
- LEROY AUTOMATION NE DEVRA PAS exiger des déclarants qu'ils établissent une relation client, concluent un accord de non-divulgation (NDA) ou contractent toute autre obligation contractuelle ou financière comme condition de réception ou de coordination d'un signalement de vulnérabilité.

Coordination avec les fournisseurs

- Si LEROY AUTOMATION détermine que la vulnérabilité signalée résulte d'une vulnérabilité affectant un produit ou service disponible de manière générale (COTS), LEROY AUTOMATION PEUT la signaler aux fournisseurs concernés, aux prestataires de services ou à des services tiers de coordination des vulnérabilités afin de permettre la correction du produit ou du service.
- LEROY AUTOMATION DEVRAIT informer les fournisseurs des vulnérabilités signalées avant toute divulgation publique.
- LEROY AUTOMATION NE DEVRA PAS révéler les informations communiquées confidentiellement par un fournisseur.
- Lorsqu'elle agit comme déclarant auprès d'autres organisations, notamment des fournisseurs ou coordinateurs, LEROY AUTOMATION DEVRA respecter les attentes applicables aux déclarants définies dans la présente politique.

Coordination avec d'autres parties

- LEROY AUTOMATION PEUT faire appel à un service tiers de coordination, tel que l'ANSSI ou l'ENISA, afin de contribuer à la résolution de tout désaccord ne pouvant être résolu entre le déclarant et LEROY AUTOMATION.
- LEROY AUTOMATION PEUT, à sa discrétion, communiquer les informations relatives à une vulnérabilité signalée à toute personne susceptible de contribuer à sa résolution et avec laquelle elle entretient une relation de confiance, notamment des fournisseurs, prestataires de services, experts de la communauté, sponsors et sites relevant d'une infrastructure critique nationale, si elle estime que ces sites sont exposés à un risque.

Divulgation publique

- LEROY AUTOMATION DEVRA déterminer la nature et le calendrier de la divulgation publique de la vulnérabilité.
- LEROY AUTOMATION PEUT divulguer au public les vulnérabilités signalées 15 jours après le signalement initial, indépendamment de l'existence ou de la disponibilité de correctifs ou de mesures de contournement proposés par les fournisseurs concernés, dans la rubrique dédiée du site web de LEROY AUTOMATION: Cybersécurité LEROY AUTOMATION
- LEROY AUTOMATION PEUT divulguer les vulnérabilités avant ou après ce délai de 15 jours en raison de circonstances exceptionnelles, notamment une exploitation active, des menaces de nature particulièrement grave ou, au contraire, mineure, ou des situations nécessitant la modification d'une norme établie.
- LEROY AUTOMATION PEUT consulter le déclarant et les fournisseurs concernés afin de déterminer le calendrier et les modalités appropriés de divulgation publique.

Politique de déclaration des déclarants

Les déclarants DOIVENT respecter les lignes directrices suivantes.

Dispositions générales

- Les déclarants DOIVENT respecter l'ensemble des lois applicables dans le cadre de leurs activités de recherche en sécurité ou de toute autre participation à ce programme de divulgation des vulnérabilités.
- Les déclarants DEVRAIENT s'efforcer de bonne foi d'informer les fournisseurs ou prestataires de services concernés et de collaborer directement avec eux avant toute divulgation publique d'un signalement de vulnérabilité.

Périmètre des tests autorisés

- Les déclarants PEUVENT tester les produits de LEROY AUTOMATION afin de détecter une vulnérabilité, dans le seul but de communiquer à LEROY AUTOMATION des informations concernant cette vulnérabilité.
- Les déclarants NE DOIVENT PAS réaliser de tests sur un produit en cours d'utilisation par un utilisateur légitime.
- Les déclarants DOIVENT déployer tous les efforts nécessaires afin d'éviter les atteintes à la vie privée, la dégradation de l'expérience utilisateur ainsi que la destruction ou la manipulation de données.
- Les déclarants DOIVENT interrompre les tests dès qu'ils ont établi l'existence d'une vulnérabilité ou rencontré des données sensibles. Les données sensibles comprennent les données à caractère personnel, les informations financières, les informations propriétaires et les secrets d'affaires.
- Les déclarants NE DOIVENT PAS exploiter une vulnérabilité au-delà du niveau minimal de test nécessaire pour démontrer son existence ou identifier un indicateur associé.
- Les déclarants NE DOIVENT PAS accéder intentionnellement au contenu des communications, données ou informations transitant par les systèmes d'information de LEROY AUTOMATION ou qui y sont stockées.
- Les déclarants NE DOIVENT PAS compromettre intentionnellement la vie privée ou la sécurité du personnel de LEROY AUTOMATION, de ses clients, du public ou de tiers légitimes.
- Les déclarants NE DOIVENT PAS exploiter les vulnérabilités découvertes afin de rebondir vers d'autres systèmes.
- Les déclarants NE DOIVENT PAS porter intentionnellement atteinte à la propriété intellectuelle ni aux autres intérêts commerciaux ou financiers des utilisateurs des produits de LEROY AUTOMATION.
- Les déclarants NE DOIVENT PAS provoquer d'indisponibilité d'un service légitime pendant leurs tests.
- Les déclarants NE DOIVENT mener aucune opération d'ingénierie sociale, sous quelque forme que ce soit, à l'encontre du personnel ou des prestataires de LEROY AUTOMATION.

Les déclarants DEVRAIENT contacter LEROY AUTOMATION à l'adresse PSIRT@leroy-agon.com s'ils ne savent pas, à un quelconque moment, s'ils peuvent poursuivre leurs tests.

Coordination avec LEROY AUTOMATION

- Les déclarants DOIVENT transmettre leurs signalements de vulnérabilité à LEROY AUTOMATION via le canal officiel PSIRT@leroy-agon.com.
- Les déclarants DEVRAIENT inclure des détails descriptifs suffisants pour permettre à LEROY AUTOMATION et, le cas échéant, aux fournisseurs concernés de reproduire précisément le comportement vulnérable.
- Les déclarants DOIVENT préserver la confidentialité de toute information relative aux vulnérabilités. Cette exigence n'empêche pas la coordination simultanée du signalement avec d'autres parties concernées, notamment des fournisseurs, prestataires de services ou coordinateurs.
- Les déclarants PEUVENT demander que leurs coordonnées ne soient pas communiquées aux fournisseurs concernés.
- Les déclarants PEUVENT demander à ne pas être nommés dans les remerciements associés aux divulgations publiques de LEROY AUTOMATION.
- Les déclarants NE DOIVENT PAS exiger de LEROY AUTOMATION qu'elle contracte une obligation contractuelle ou financière comme condition de transmission d'un signalement de vulnérabilité.
- Les déclarants NE DOIVENT PAS exiger de rémunération en contrepartie du signalement d'une vulnérabilité effectué en dehors d'un programme explicite de bug bounty.

Coordination avec les fournisseurs

Lorsqu'un déclarant découvre, dans un produit LEROY AUTOMATION, une vulnérabilité résultant d'une vulnérabilité affectant un produit ou service disponible de manière générale, il PEUT la signaler aux fournisseurs concernés, aux prestataires de services ou à un service tiers de coordination des vulnérabilités, sans divulguer d'informations sensibles concernant le produit LEROY AUTOMATION, afin de permettre la correction du produit ou du service.

Coordination avec d'autres parties

Les déclarants NE DEVRAIENT divulguer aucun détail, quelle qu'en soit l'étendue, concernant une vulnérabilité affectant un produit LEROY AUTOMATION, ni aucun indicateur de vulnérabilité, à une partie qui n'en avait pas déjà connaissance au moment où le signalement est transmis à LEROY AUTOMATION.

Divulgation publique

- Les déclarants PEUVENT divulguer publiquement l'existence antérieure de vulnérabilités déjà corrigées par LEROY AUTOMATION, notamment des informations potentielles sur la vulnérabilité, des indicateurs de vulnérabilité ou la nature, mais non le contenu, des informations auxquelles la vulnérabilité a donné accès.
- Les déclarants qui choisissent une divulgation publique DEVRONT procéder en concertation avec LEROY AUTOMATION.
- Les déclarants NE DOIVENT PAS divulguer à une partie qui n'en avait pas déjà connaissance lors du signalement à LEROY AUTOMATION les données propriétaires découvertes fortuitement pendant les tests ni le contenu des informations rendues accessibles par la vulnérabilité.

Annexe 1: Fiche de divulgation

Contact : Vous devez envoyer les informations découvertes exclusivement à l'adresse e-mail suivante : PSIRT@leroy-agon.com .
Dans la mesure du possible, nous vous invitons à utiliser la méthode de communication sécurisées PGP avec les informations suivantes :

ID de clé PGP : 1668FD92
Type de Clé PGP : Clé RSA-4096
Empreinte digitale de la clé PGP : A7B9 E8AA F0AA AF13 C13D 3524 3FBC 9FC1 1668 FD92

Nous vous demandons de fournir au moins les informations pertinentes suivantes :

Nom de famille : Prénom :	
Adresse électronique : Numéro de téléphone : Adresse :	
Description de la vulnérabilité:	
Type de vulnérabilité:	
Détails de configuration:	
Opérations effectuées (journaux) :	
Outils utilisés:	
Dates et heures des tests:	
Toute autre information pertinente:	