Politique de divulgation des vulnérabilités

Signalement responsable, investigation et correction des vulnérabilités de sécurité

Version	Date d'entrée en vigueur	Responsable du document	Contact
1.0	Septembre 2026	Équipe de sécurité SALUS Controls PLC	security@saluscontrols.com

1. Introduction

SALUS Controls PLC s'engage à protéger la sécurité de ses produits, services et clients. Nous accueillons les signalements responsables de clients, chercheurs en sécurité, partenaires, développeurs et autres membres de la communauté de la sécurité qui identifient des vulnérabilités potentielles affectant les produits ou services de SALUS Controls PLC.

Notre objectif est d'examiner rapidement les signalements de vulnérabilités potentielles, de communiquer de manière appropriée avec la partie déclarante tout au long du processus et de mettre en œuvre des mesures de correction ou d'atténuation proportionnées afin de protéger les utilisateurs.

Signalez les vulnérabilités potentielles de sécurité de manière confidentielle à security@saluscontrols.com. SALUS Controls PLC accusera réception dans un délai de trois jours ouvrés et, dans tous les cas, au plus tard dans les sept jours calendaires. Cet accusé confirme uniquement la réception des informations et ne signifie pas que le problème signalé a été confirmé comme vulnérabilité.

2. Champ d'application

La présente politique s'applique aux vulnérabilités de sécurité affectant :

- Les produits SALUS Controls PLC
- Les micrologiciels et logiciels
- Les applications mobiles
- Les services cloud
- Les applications web et sites internet accessibles au public

Pour toute question concernant l'installation, la configuration, la garantie ou tout autre sujet non lié à la sécurité, veuillez contacter notre service client via les canaux d'assistance habituels.

Nous acceptons les signalements de sécurité concernant les produits SALUS quel que soit leur statut dans le cycle de vie. Pour les produits encore couverts par leur période de support de sécurité publiée, les vulnérabilités et mises à jour de sécurité sont traitées conformément aux obligations légales applicables. Pour les produits hors de cette période, SALUS Controls PLC continuera d'évaluer les signalements et pourra proposer des mesures d'atténuation, des conseils de migration ou d'autres recommandations selon le risque, la faisabilité technique et les obligations applicables.

3. Signaler une vulnérabilité

Si vous pensez avoir identifié une vulnérabilité de sécurité, veuillez la signaler de manière confidentielle par e-mail à **security@saluscontrols.com**

Les signalements peuvent être soumis anonymement. L'absence de nom ou de moyen de contact bidirectionnel n'empêchera ni leur réception ni leur évaluation initiale, mais pourra limiter notre capacité à demander des informations complémentaires, fournir des mises à jour de statut ou proposer une reconnaissance publique.

Nous acceptons un premier signalement envoyé par e-mail ordinaire ou par un autre canal. Si du code d'exploitation, des identifiants, des données personnelles, des configurations client ou d'autres informations sensibles doivent être échangés, SALUS Controls PLC proposera une méthode sécurisée disponible pour poursuivre les échanges. L'impossibilité ou le choix de la partie déclarante de ne pas utiliser le chiffrement ne conduira pas, à lui seul, au rejet du signalement.

4. Informations à fournir

Afin de nous aider à examiner efficacement votre signalement, veuillez inclure, si possible :

- Nom et modèle du produit
- Version du micrologiciel ou du logiciel
- Description de la vulnérabilité
- Étapes permettant de reproduire le problème
- Comportement attendu et comportement observé
- Impact potentiel sur la sécurité
- Captures d'écran, journaux ou preuve de concept, si disponibles
- Vos coordonnées de contact préférées pour le suivi

Veuillez éviter d'inclure des informations personnelles sensibles sauf si elles sont nécessaires pour démontrer la vulnérabilité.

Veuillez également indiquer, si vous le savez, si le problème est public, activement exploité, a affecté des utilisateurs ou a été signalé à un autre fournisseur, prestataire ou coordinateur. Il n'est pas nécessaire de fournir toutes les informations demandées pour que nous acceptions et enregistrions un signalement.

Lors d'une divulgation coordonnée, l'accès aux informations non publiques sur les vulnérabilités est limité aux personnes qui doivent en avoir connaissance. SALUS Controls PLC peut partager les informations nécessaires avec les équipes produit, fournisseurs, coordinateurs, parties concernées ou autorités compétentes afin de valider et corriger le problème, protéger les utilisateurs et respecter les obligations légales, sous réserve de mesures appropriées de confidentialité et de protection des données.

Les données personnelles transmises avec un signalement de vulnérabilité sont traitées conformément à la politique de confidentialité applicable de SALUS Controls PLC. Consultez :https://saluscontrols.com/fr/politique-confidentialite-cookies/

5. Processus de réponse

Après réception de votre signalement, SALUS Controls PLC :

- Accusera réception dans un délai de trois jours ouvrés et, dans tous les cas, au plus tard sous sept jours calendaires ; si possible, avec un identifiant de dossier unique et des informations préliminaires sur son statut.
- Effectuera une évaluation initiale dans un délai de sept jours ouvrés
- Validera la vulnérabilité signalée
- Évaluera sa gravité et son impact potentiel
- Élaborera, le cas échéant, un plan de correction ou une mise à jour de sécurité
- Vous tiendra informé tout au long de l'investigation et du processus de correction
- Tant qu'un dossier reste actif, fournira une mise à jour substantielle au moins tous les 30 jours calendaires et communiquera plus tôt en cas de changement significatif du périmètre confirmé, du risque, de l'approche de correction ou de la date de divulgation.
- Si des informations supplémentaires sont nécessaires, nous pourrons vous contacter pendant notre investigation.

6. Correction fondée sur le risque

Les vulnérabilités confirmées sont priorisées selon leur gravité technique, leur exploitabilité, les produits concernés, l'impact potentiel, l'exposition des utilisateurs, les preuves d'exploitation active, les mesures d'atténuation disponibles et les exigences d'un déploiement sûr. Un score numérique peut contribuer à l'évaluation, mais ne détermine pas à lui seul la priorité de correction.

SALUS Controls PLC fixe un objectif de correction propre à chaque dossier et communique les changements importants à la partie déclarante. Lorsqu'une correction immédiate n'est pas possible, des mesures d'atténuation ou des recommandations de réduction du risque peuvent être fournies avant qu'une solution permanente ne soit disponible.

7. Divulgation coordonnée des vulnérabilités

SALUS Controls PLC collabore avec la partie déclarante et, si nécessaire, les fournisseurs, coordinateurs et autres parties concernées afin de fixer une date de divulgation propre au dossier. Le calendrier peut être révisé selon la gravité, l'exploitation active, le risque pour les utilisateurs, l'avancement de la correction et du déploiement, les dépendances de la chaîne d'approvisionnement et les obligations légales ou réglementaires applicables. Toute modification importante de la date cible sera communiquée aux parties concernées.

SALUS Controls PLC peut accélérer l'information des utilisateurs ou la divulgation publique lorsqu'une vulnérabilité est déjà publique, activement exploitée, présente un risque urgent pour les utilisateurs, est susceptible d'être divulguée ou lorsque la loi impose une notification. Lorsqu'une correction complète n'est pas encore disponible, SALUS peut fournir des mesures temporaires d'atténuation ou de réduction du risque sans faciliter inutilement l'exploitation.

Les informations sur les vulnérabilités corrigées seront publiées dans des avis de sécurité accessibles et lisibles. Ces avis préciseront la vulnérabilité et les produits concernés, les dates de publication et de révision, l'impact potentiel et la gravité, les corrections ou mesures d'atténuation disponibles, les actions requises des utilisateurs et les coordonnées de contact. Les avis concernant des composants tiers peuvent renvoyer à des informations de référence lorsque cela permet aux utilisateurs de déterminer si les produits SALUS sont concernés.

Les informations sur les vulnérabilités seront également mises à disposition dans un format lisible par machine largement reconnu, sauf si une justification contraire est documentée et approuvée. La publication ne peut être retardée ou omise que lorsque les conditions applicables ont été évaluées, documentées et approuvées.

Lorsque la loi applicable l'exige ou lorsque cela est nécessaire pour protéger les utilisateurs, SALUS Controls PLC informera les utilisateurs concernés et fournira les mesures d'atténuation ou recommandations correctives disponibles via des canaux appropriés et accessibles.

8. Support des mises à jour de sécurité

SALUS Controls PLC fournit des mises à jour de sécurité pendant toute la période de support définie pour chaque produit concerné. Cette période est déterminée conformément aux exigences légales applicables, en tenant compte de la durée d'utilisation prévue du produit, de sa nature et des attentes raisonnables des utilisateurs.

La période de support sera d'au moins cinq ans, sauf si une durée d'utilisation plus courte du produit est raisonnablement attendue, et pourra être plus longue si la durée de vie prévue du produit le justifie. La date de fin de la période de support applicable sera communiquée dans les informations relatives au produit.

9. Hors champ

Tous les signalements potentiels de sécurité sont enregistrés et font l'objet d'une évaluation initiale. Les problèmes purement fonctionnels, commerciaux ou liés au support peuvent être redirigés vers le canal d'assistance approprié. Si un problème ne peut pas être reproduit initialement, SALUS Controls PLC peut demander des informations supplémentaires et réévaluer le signalement lorsque de nouveaux éléments sont disponibles.

Les problèmes théoriques, scénarios nécessitant un accès physique, situations de déni de service, scénarios d'ingénierie sociale et dépendances tierces sont évalués selon leur impact réaliste sur la sécurité, leur exploitabilité et l'utilisation prévue et raisonnablement prévisible du produit.

Les vulnérabilités affectant des composants tiers intégrés à un produit SALUS, fournis avec celui-ci ou dont il dépend restent soumises à l'évaluation de l'impact sur le produit par SALUS.

10. Recherche responsable en sécurité

SALUS Controls PLC soutient la recherche responsable en sécurité menée de bonne foi. Nous demandons aux chercheurs de :

- Agir de manière responsable et éthique

- Éviter de perturber les produits, services ou activités des clients
- Éviter d'accéder aux données des clients, de les modifier ou de les supprimer
- Signaler les vulnérabilités de manière confidentielle selon le processus décrit dans cette politique
- Accorder à SALUS Controls PLC un délai raisonnable pour examiner et corriger le problème avant toute divulgation publique
- Respecter toutes les lois et réglementations applicables lors des recherches en sécurité

Lorsqu'une partie déclarante agit de bonne foi, respecte cette politique, évite tout préjudice et signale rapidement le problème, SALUS Controls PLC n'a pas l'intention d'engager une action en justice uniquement en raison d'une recherche en sécurité menée conformément à cette politique. Cette déclaration n'autorise pas l'accès aux systèmes ou données de tiers, n'engage aucun tiers ni aucune autorité et ne dispense pas la partie déclarante de respecter la loi applicable et d'obtenir les autorisations nécessaires.

11. Contact

Pour tout signalement lié à la sécurité ou toute question concernant cette politique, veuillez contacter :

Équipe de sécurité SALUS Controls PLC

E-mail : security@saluscontrols.com**security@saluscontrols.com**

12. Mise à jour de la politique

Cette politique est révisée au moins une fois par an et après toute modification importante des exigences légales applicables, des canaux de signalement, du périmètre des produits ou des processus de gestion des vulnérabilités. La version actuelle, la date de publication, la date de dernière mise à jour et le responsable de la politique sont affichés avec la politique publiée.

13. Remerciements

Avec le consentement de la partie déclarante, SALUS Controls PLC peut mentionner le nom, le pseudonyme ou l'organisation d'une partie ayant soumis un signalement de vulnérabilité valide et contribué à une divulgation coordonnée. Les signalements peuvent être anonymes et le refus d'être mentionné n'affecte ni l'acceptation, ni la priorisation, ni les décisions de correction.

Cette politique ne constitue pas un programme de bug bounty et ne garantit aucune récompense financière ou autre.