

SALUS Controls PLC - Formulaire de signalement d'une vulnérabilité suspectée

Utilisez ce formulaire pour signaler une vulnérabilité de sécurité suspectée affectant un produit, une application, un service cloud ou un site web de SALUS.

Veuillez fournir autant d'informations que possible. Il n'est pas nécessaire de remplir tous les champs pour que nous puissions accepter votre signalement.

Vous pouvez effectuer un signalement de manière anonyme. Toutefois, si vous ne fournissez pas vos coordonnées, nous pourrions ne pas être en mesure de vous demander des informations complémentaires ni de vous tenir informé(e) du suivi de votre signalement.

Une fois rempli, veuillez envoyer ce formulaire à security@saluscontrols.com.

Veuillez ne pas inclure de mots de passe, de jetons d'authentification, de clés privées ni de données personnelles ou clients non nécessaires.

Les champs indiqués « Obligatoire » ne sont requis que lorsque les informations sont raisonnablement disponibles. Si vous ne disposez pas de toutes les informations, vous pouvez tout de même envoyer votre signalement.

Signalement d' une vulnérabilité suspectée

1. Informations sur l' auteur du signalement

Champ	Réponse
Nom ou pseudonyme (facultatif)	
Organisation (facultatif)	
E-mail/moyen de contact (obligatoire sauf signalement anonyme)	
Langue préférée (facultatif)	
Signalement anonyme ?	☐ Oui ☐ Non

2. Produit ou composant concerné

Champ	Réponse
Nom du produit ou service (obligatoire)	
Modèle (le cas échéant)	
Version matérielle (si connue)	

Champ	Réponse
Version du firmware / logiciel / application (si connue)	
Pays / région	
Autres informations de configuration pertinentes	

3. Description de la vulnérabilité suspectée

Champ	Réponse
Titre court (obligatoire)	
Veuillez décrire le problème de sécurité identifié (obligatoire)	
Quand avez-vous constaté le problème pour la première fois ?	
Quel comportement attendiez-vous ?	
Que s'est-il réellement passé ?	
Pouvez-vous reproduire le problème ?	☐ Oui ☐ Non ☐ Parfois ☐ Inconnu
Si possible, décrivez les étapes nécessaires pour le reproduire :	
Selon vous, quel impact ce problème pourrait-il avoir sur la sécurité ?	
Pièces jointes incluses ? Vous pouvez fournir des captures d'écran, journaux, vidéos ou informations de preuve de concept pertinents.	☐ Oui ☐ Non

Informations techniques complémentaires (facultatif – pour les chercheurs en sécurité)

Champ	Réponse
Type de vulnérabilité (contournement de l'authentification, injection, corruption de mémoire, etc.), si connu	
CWE / CVE, si connu	
Cause technique / détails	

Champ	Réponse
Environnement de test / configuration	
Preuve de concept	

4. Scénario d'attaque

Le scénario d'attaque est différent de la procédure de reproduction. Décrivez comment un attaquant pourrait, dans un cas réaliste, exploiter le problème.

Champ	Réponse
Si vous le savez, veuillez décrire comment une personne pourrait exploiter cette vulnérabilité	
Accès requis pour l'attaquant	☐ Réseau distant ☐ Réseau adjacent ☐ Réseau local ☐ Local device ☐ Physical access ☐ Inconnu
Interaction de l'utilisateur requise	☐ Oui ☐ Non ☐ Inconnu
Autorisations spéciales / compte requis	☐ Oui ☐ Non ☐ Inconnu Si oui, veuillez décrire les autorisations / le compte requis :

5. Évaluation de l'impact (facultatif)

Remplissez cette section si vous êtes en mesure d'évaluer l'impact potentiel.

Domaine d'impact	Évaluation par l'auteur du signalement
Confidentialité	☐ Aucun ☐ Faible ☐ Moyen ☐ Élevé ☐ Inconnu
Intégrité	☐ Aucun ☐ Faible ☐ Moyen ☐ Élevé ☐ Inconnu
Disponibilité	☐ Aucun ☐ Faible ☐ Moyen ☐ Élevé ☐ Inconnu
Sécurité des personnes et des biens	☐ Aucun ☐ Faible ☐ Moyen ☐ Élevé ☐ Inconnu
Vie privée	☐ Aucun ☐ Faible ☐ Moyen ☐ Élevé ☐ Inconnu

Domaine d' impact	Évaluation par l' auteur du signalement
Impact sur la chaîne d'approvisionnement ou l'écosystème au sens large	☐ Aucun ☐ Faible ☐ Moyen ☐ Élevé ☐ Inconnu
Niveau de gravité suggéré, si disponible (facultatif)	☐ Faible ☐ Moyen ☐ Élevé ☐ Critique ☐ Inconnu
Vecteur CVSS, si disponible (facultatif)	

6. État de l'exploitation et de la divulgation

Champ	Réponse
La vulnérabilité est-elle déjà publique ?	☐ Non ☐ Oui ☐ Inconnu Si oui, veuillez indiquer l'URL et la date :
Une preuve de concept est-elle publique ?	☐ Non ☐ Oui ☐ Inconnu Si oui, veuillez indiquer l'URL et la date :
Une exploitation active est-elle connue ou suspectée ?	☐ Non ☐ Oui ☐ Inconnu Si oui, veuillez fournir des précisions :
Un autre fournisseur, prestataire, CERT ou coordinateur a-t-il été contacté ?	☐ Non ☐ Oui ☐ Inconnu ☐ ☐ Si oui, veuillez indiquer l'organisme, l'identifiant du dossier et la date :
Prévoyez-vous d' évoquer ou de publier le problème après sa correction ?	☐ Non ☐ Oui ☐ Inconnu Si oui, veuillez fournir des précisions :
Date souhaitée de divulgation coordonnée, le cas échéant	

Note relative à la divulgation coordonnée : security@saluscontrols.com

Veuillez conserver confidentielles les informations non publiques relatives à la vulnérabilité jusqu'à la date de divulgation convenue. Si le niveau de risque évolue, si une exploitation active est observée ou si une divulgation publique devient probable, veuillez contacter rapidement security@saluscontrols.com afin que le plan de divulgation puisse être réévalué.

7. Mesures correctives ou d'atténuation suggérées (facultatif)

- Correction de la cause première suggérée, si connue : _____
- Mesure d' atténuation temporaire ou solution de contournement suggérée, si connue : _____
- Bonne pratique du secteur, règle de défense ou référence pertinente : _____

8. Préférence concernant la mention publique

Choix	Réponse
Pouvons-nous vous mentionner publiquement si un avis de sécurité est publié ?	☐ Oui ☐ Non
Nom affiché, pseudonyme ou organisation	
Lien de profil ou de référence souhaité, s' il est accepté par la politique	

9. Pièces jointes et informations complémentaires

Veuillez indiquer les fichiers joints à votre signalement. N'incluez pas de mots de passe, de jetons d'authentification, de clés privées ni de données personnelles ou clients non nécessaires.

Champ	Réponse
Des fichiers sont-ils joints à ce signalement ?	☐ Oui ☐ Non
Type de fichiers joints	☐ Captures d'écran ☐ Journaux ☐ Vidéo ☐ Preuve de concept ☐ Capture de paquets ☐ Autre
Description des fichiers joints	
Informations complémentaires pertinentes pour le signalement	
Exigences de confidentialité ou de traitement	

Si vous joignez des journaux, captures d'écran, vidéos, captures de paquets ou éléments de preuve de concept, veuillez supprimer les données personnelles ou clients non nécessaires, les mots de passe, les jetons d'authentification, les clés privées ou toute autre information sensible avant d'envoyer le signalement.

10. Confirmation de bonne foi

En envoyant ce signalement, son auteur confirme, à sa connaissance, que :

- ☐ Le signalement est exact et les informations ont été obtenues dans le cadre de recherches de sécurité menées de bonne foi.
- ☐ Les tests ont été limités aux systèmes, appareils, comptes et données appartenant à l' auteur du signalement ou pour lesquels il était autorisé à effectuer des tests.
- ☐ Tout accès, conservation ou divulgation non nécessaire de données non publiques a été évité.
- ☐ L' auteur du signalement coordonnera la divulgation conformément à la politique publiée, sous réserve de la législation applicable et de toute évolution urgente du risque pour les utilisateurs.

☐ Je confirme ne pas avoir intentionnellement inclus de mots de passe, de jetons d'authentification, de clés privées ni de données personnelles ou clients non nécessaires.

Date d' envoi : _____

Nom ou pseudonyme de l' auteur du signalement, le cas échéant :

Comment envoyer ce signalement

Veuillez envoyer le formulaire rempli par e-mail à : security@saluscontrols.com

Vous pouvez également signaler une vulnérabilité suspectée directement par e-mail, sans utiliser ce formulaire. L'utilisation de ce formulaire est recommandée, car elle aide SALUS Controls PLC à recueillir les informations nécessaires pour évaluer efficacement le signalement.