POLITIQUE DE DIVULGATION RESPONSABLE

Le Groupe Carrus reconnaît l'importance de la sécurité de l'information pour nos clients et nous sommes déterminés à maintenir un niveau élevé de transparence et d'intégrité dans toutes nos activités. C'est pourquoi nous avons mis en place une politique de divulgation responsable qui vise à encourager et à faciliter le signalement responsable de toute vulnérabilité ou incident de sécurité lié à nos systèmes.

L'objectif de cette politique est de permettre à nos clients et à toute personne découvrant une vulnérabilité technique potentielle dans nos produits, services et systèmes de la signaler de manière responsable, afin que des mesures correctives puissent être prises rapidement pour garantir la sécurité de nos solutions de gestion de paris.

1. Signalisation de vulnérabilité

- Signalez la vulnérabilité dès que possible après sa découverte via l'assistance opérationnelle (asop@groupecarrus.com) disponible tous les jours.
- Donnez-nous suffisamment d'informations pour reproduire le problème. Ainsi, nous pourrons résoudre le problème le plus rapidement possible. De manière générale, l'adresse IP ou l'URL du système affecté et une description de la vulnérabilité suffisent. En cas de vulnérabilités plus complexes, des informations supplémentaires peuvent être nécessaires ; nous vous demanderons dans ce cas de nous fournir plus d'informations.
- Indiquez vos coordonnées (adresse e-mail ou numéro de téléphone) afin que nous puissions vous contacter.
- Ne partagez pas les informations relatives au problème de sécurité avec d'autres personnes avant que nous ayons pu résoudre le problème.

2. Champ d'application des vulnérabilités

Les vulnérabilités techniques des produits, services et systèmes du Groupe Carrus relèvent de notre programme de sécurité.

Les vulnérabilités énumérées ci-dessous sont hors champ d'application :

- Vulnérabilités liées aux attaques par déni de service (DoS).
- Vulnérabilités découvertes à l'aide d'outils automatisés ou d'analyses.
- Vulnérabilités nécessitant un accès physique à l'ordinateur ou au périphérique d'un utilisateur.
- Spam ou techniques d'ingénierie sociale.
- Attaques physiques contre les bureaux ou les centres de données du Groupe Carrus.

3. Traitements

Suite à votre signalement,

- Vous recevrez une confirmation de réception de votre alerte dans un délai d'un jour ouvrable.
- Nous répondrons à votre alerte dans un délai de cinq jours ouvrables. Notre réponse contient une évaluation de la vulnérabilité et une date prévue pour proposer une solution.
- Nous vous tiendrons informés en tant que rapporteur de l'évolution du problème.
- Nous traitons votre signalement de manière confidentielle et nous ne partageons pas vos données personnelles sans votre autorisation avec des tiers, sauf si la loi ou une décision de justice nous y oblige.
- Nous résoudrons le problème de sécurité signalé le plus rapidement possible. Nous rapporterons le problème si nécessaire uniquement après l'avoir résolu.

Le Groupe Carrus se réserve, par ailleurs, le droit de mettre à jour la présente Politique de divulgation responsable à tout moment.