Rédigé : 2021-06-01	**Section :** **Sous-section :**	CYBERSÉCURITÉ ET TÉLÉCOM CYBERSÉCURITÉ	**Émetteur :** Cybersécurité
Remplace : N/A	**Sujet :**	Directive de divulgation responsable des vulnérabilités de sécurité	**Approuvé :** 7 décembre 2021 **En vigueur :** 7 décembre 2021

CONTEXTE

La Société des alcools du Québec (SAQ) accepte la divulgation responsable des problèmes de sécurité trouvés sur ses sites web, ses applications ainsi que ses infrastructures informatiques, incluant les infrastructures infonuagiques. Nous avons à cœur la protection des données personnelles des Québécois et apprécions le support de la communauté pour nous aider dans cette mission.

La SAQ reconnaît que la communauté des experts en sécurité peut favoriser l'augmentation de la posture de sécurité de la SAQ.

Cependant, compte tenu de la mission de nos systèmes, cela ne signifie pas que la SAQ cautionne ou autorise l'utilisation de techniques de recherches actives de problèmes de sécurité durant les heures de grand achalandage. La SAQ a en place des procédures adéquates pour ce type d'activités.

CONSIGNES RELATIVES AUX ACTIONS DE BONNE FOI

La présente directive a pour but de baliser la façon d'investiguer et de divulguer les brèches.

1) Sous réserve des autres conditions mentionnées dans la présente directive, la SAQ n'engagera aucune poursuite contre une personne ayant détecté des failles usant de bonne foi et prenant des moyens raisonnables afin de prévenir la publication, l'altération de données ou l'accessibilité des différents services de la SAQ.
2) Dans le cas d'une faille de sécurité où des données personnelles peuvent être accessibles, veuillez nous contacter immédiatement, et cesser vos activités.
3) La SAQ n'accepte pas que vous, stockiez, fassiez l'extraction de données.
4) Vous ne devrez jamais publier les données non publiques de la SAQ que vous aurez obtenues lors de vos investigations.
5) Nous visons une réponse via courriel dans les 72 heures suivant la divulgation de la faille à nos équipes. Nous visons également un délai de 72 heures pour répondre si vous rapportez une faille

pouvant entraîner l'exécution de code distant. Pour les problèmes mineurs, une réponse sera envoyée en 7 jours calendrier.

6) À la suite de l'analyse de la faille, nos équipes communiquerons au besoin avec vous afin d'établir un calendrier où les détails de la faille pourront être rendus publics.
7) Toute attaque réussie de votre part doit nous être rapportée à l'intérieur de 7 jours calendrier à l'adresse ci-dessous.
8) Toute tentative de chantage entraînera des recours judiciaires.
9) La démonstration des problèmes de sécurité doit se faire uniquement dans le but de prouver qu'une faille est présente.

   Voici des exemples d'actions qui pourront entraîner des recours judiciaires (cette liste n'est pas limitative) :

   a. Extraction d'une grande partie d'une base de données;
   b. Établissement de mécanismes de persistance sur des systèmes;
   c. Si une exploitation est réussie, reconnaissance à l'intérieur de notre réseau;
   d. Si une exploitation est réussie, mouvement latéral à l'intérieur de notre réseau;
   e. Si une exploitation est réussie, utilisation d'outil d'extraction de mots de passe (par ex. : Mimikatz);
   f. Publication de données personnelles ou confidentielles sur Internet;
   g. Altération de données à grande échelle;
   h. Dénis de service par engorgement;
   i. Utilisation frauduleuse des informations obtenues;
   j. Utilisation d'hameçonnage, ingénierie sociale.

RÉCOMPENSE

Vous n'exigerez aucune contrepartie pour votre intervention.

PROCÉDURES DE DIVULGATION RESPONSABLE/DE VULNÉRABILITÉ COMMENT SIGNALER UNE VULNÉRABILITÉ

Toute divulgation doit être envoyée à l'adresse courriel suivante : **divulgation-securite@saq.qc.ca**. Aucun accusé de réception ne sera automatiquement transmis. Afin de pouvoir reproduire et valider la potentielle vulnérabilité, nous apprécierions recevoir les informations suivantes :

1. La date, l'heure, le fuseau horaire et l'adresse source du test;
2. Le ou les systèmes ciblés, par exemple : adresse IP, numéro de port, URL;
3. La classe d'attaque : injection, vulnérabilité connue (CVE-) ;
4. Description de l'attaque, éventuellement charge utile (c.-à-d.: payload) et outils utilisés et les étapes pour la reproduire.
5. Copie d'écran ou logs; le cas échéant, le type de données accessibles.