Régie de l'assurance maladie Québec

Infolettre RAMQ

5 mai 2021
036

> Développeurs de logiciels – Médecine
> Développeurs de logiciels – Pharmacie
> Développeurs de logiciels – Optométrie et dentisterie
> Établissements et laboratoires d'aides techniques

Protocole TLS : Report de la fin du support des versions 1.0 et 1.1

1 Rappel

Dans l'infolettre 205 du 21 octobre 2020, l'infolettre 062 du 12 mai 2020 et l'infolettre 324 du 17 février 2020, nous vous annoncions notre intention de mettre fin au support des versions 1.0 et 1.1 du protocole TLS (Transport Layer Security).

Dans l'infolettre 348 du 18 mars 2021, nous vous avons invité à faire des essais dans l'environnement Partenaire entre le 6 et le 23 avril 2021 afin de valider vos communications par mesure de précaution avant le retrait des anciens protocoles TLS 1.0 et 1.1.

À la suite de cette dernière infolettre, nous avons communiqué de nouveau avec vous pour vous informer que la RAMQ avait procédé le 1er avril dernier au remplacement d'une composante technologique dans son infrastructure réseau (balanceur de charge) dans l'environnement Partenaire. En fait, cette étape était préalable au retrait des protocoles TLS version 1.0 et 1.1.

Même si ce changement devait être transparent lors de vos essais de communication, certains d'entre vous ont rencontré quelques problèmes (maintenant résolus) à venir faire des essais de communication. Nous avons donc prolongé la période jusqu'au 30 avril.

2 Remplacement des balanceurs de charge

Nous vous informons que nous procéderons au remplacement de la même composante technologique (balanceurs de charge) dans l'environnement Production dans la nuit du 21 au 22 mai prochain à partir de 23 h.

Pour les partenaires externes qui n'auraient pas encore effectué d'essais dans l'environnement Partenaire, il est important de tenir compte des informations et des recommandations techniques suivantes.

2.1 Mise en contexte

- Dans les communications réseautiques, en plus de préciser la version du protocole TLS utilisée (ex. TLS1.2), il est aussi requis de mentionner les algorithmes d'encryptage permis.
- Les nouveaux et les anciens balanceurs de charge utilisés à la RAMQ supportent les mêmes protocoles TLS (ex. TLS1.2), mais pas nécessairement tous les mêmes algorithmes d'encryptage (appelés CIPHER).
- La configuration des nouveaux balanceurs de charge mise sur l'utilisation de CIPHER plus robustes et plus récents que ceux avec les anciens balanceurs de charge.
    - Cette situation a provoqué un problème pour les partenaires externes qui ont renforcé leurs communications en utilisant des CIPHER plus robustes, mais qui ne sont pas supportés par les anciens balanceurs de charge de la RAMQ qui ont encore une utilisation en PROD.

2.2 Solution

Les partenaires externes qui sont dans cette situation devraient donc miser sur l'utilisation de CIPHER compatibles avec les anciens et les nouveaux balanceurs de charge utilisés à la RAMQ.

- **Solution :** Inclure dans les communications réseaux avec la RAMQ au moins un CIPHER présent dans la colonne de gauche **et** au moins un CIPHER de la colonne de droite de la liste suivante.

  Ainsi, ils pourront communiquer avec succès avec la RAMQ dans les différents environnements quels que soient les balanceurs de charge utilisés (anciens ou nouveaux balanceurs).

HAPROXY (nouveaux balanceurs)	Cisco ACE (anciens balanceurs)
ECDHE-RSA-AES256-GCM-SHA384	RSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384	RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-AES256-SHA384	RSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES256-SHA384	
ECDHE-RSA-AES256-SHA	
ECDHE-ECDSA-AES256-SHA	
DHE-RSA-AES256-GCM-SHA384	
DHE-RSA-AES256-GCM-SHA	
DHE-RSA-AES256-SHA256	
DHE-RSA-AES256-SHA	

3 Suite

Après le changement des balanceurs de charge en environnement de production prévu le 21 mai prochain, la RAMQ sera en mesure de planifier la désactivation des anciens protocoles TLS 1.0 et 1.1.

Nous vous tiendrons informés dans une prochaine infolettre du moment de la désactivation des versions 1.0 et 1.1 de TLS dans les deux environnements : Partenaire et Production.

Nous vous remercions de votre collaboration.