Guide rapide :

préparez vos systèmes pour le roulement de la KSK de la racine

Qu'est-ce que le roulement de la KSK de la racine ?

La Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) a l'intention de réaliser un roulement, ou modifier, la paire « principale » de clés cryptographiques utilisée dans le protocole des extensions de sécurité du système des noms de domaine (DNSSEC), communément dénommée la clé de signature de clé (KSK) de la zone racine. Ce sera la première fois que la KSK aura été changée depuis qu'elle a été initialement générée en 2010. C'est un pas important vers la sécurité, tout comme la modification régulière des mots de passe est considérée comme une pratique prudente par les utilisateurs de l'Internet.

Changer la clé implique la génération d'une nouvelle paire de clés cryptographiques et la distribution de la nouvelle clé publique aux résolveurs validant DNSSEC. Étant donné que chaque requête Internet utilisant DNSSEC dépend de la KSK de la zone racine pour valider sa destination, cela constituera un changement marquant. Maintenant que la nouvelle clé a été générée, les opérateurs, tels que les FSI, devront mettre à jour leurs systèmes avec la nouvelle clé de sorte que lorsqu'un utilisateur tente de se rendre sur un site Web, ces opérateurs puissent valider la requête en utilisant la nouvelle KSK.

Pourquoi il vous faut vous préparer

À l'heure actuelle, environ un quart des internautes dans le monde a accès à Internet via des résolveurs validant DNSSEC sur lesquels le roulement de la KSK pourrait avoir des répercussions. Si ces résolveurs de validation n'ont pas la nouvelle clé lors du roulement de la KSK, les utilisateurs finaux qui les utilisent rencontreront des erreurs et ne pourront pas accéder à l'Internet.

Si vous n'utilisez pas les DNSSEC, le roulement n'aura pas de conséquences pour votre système. Sachez toutefois que les DNSSEC constituent un élément important de la prévention de l'usurpation de nom de domaine.

L'ICANN propose une plateforme d'essai pour les opérateurs de réseau et autres parties souhaitant s'assurer que leurs systèmes peuvent gérer correctement le processus de mise à jour automatique. Vérifiez que vos systèmes sont prêts à l'adresse suivante : **https://go.icann.org/KSKtest**.

Si vous avez permis la validation DNSSEC, vous devez mettre à jour vos systèmes avec la nouvelle KSK pour aider à assurer l'accès de vos utilisateurs à Internet.

Conçu par le département des communications de l'ICANN | mars 2018

Ce qu'il faut faire

Vos systèmes peuvent être mis à jour à tout moment avant le roulement en utilisant la nouvelle KSK de la zone racine qui a été publiée le 11 juillet 2017. Certains systèmes ont probablement déjà des mises à jour automatisées en place. Les mesures qu'il vous faut prendre dépendent de ce qui suit :

Si votre logiciel permet les mises à jour automatisées des ancres de confiance du DNSSEC(RFC 5011) :

La KSK aurait dû être mise à jour automatiquement, le moment venu. Il n'est pas nécessaire de prendre d'autres mesures.

Notons que les dispositifs qui sont hors ligne au cours du roulement devront être mis à jour manuellement s'ils sont mis en ligne une fois que le roulement est terminé.

L'ICANN a commencé à proposer un banc d'essai en mars 2017 pour les opérateurs ou toute autre partie souhaitant s'assurer que leurs systèmes peuvent gérer correctement le processus de mise à jour automatique. De plus amples informations sont disponibles sur : **icann.org/kskroll.**

Si votre logiciel ne permet pas la mise à jour automatisée des ancres de confiance des DNSSEC (RFC 5011) ou n'est pas configuré pour l'utiliser :

L'ancre de confiance du logiciel doit être mise à jour manuellement. La nouvelle KSK de la zone racine est disponible ici : **https://go.icann.org/2DOB7zn**.

Quand le roulement de la KSK aura-t-il lieu ?

Le roulement de la KSK est un processus, pas un seul événement. Les dates suivantes représentent des jalons clés de ce processus, moments auxquels les utilisateurs finaux pourraient rencontrer une interruption des services Internet :

11 octobre 2018

Date à laquelle la nouvelle KSK sera utilisée à des fins de signature pour la première fois.

11 janvier 2019

Date à laquelle l'ancienne KSK cessera de fonctionner.

De plus amples informations sur le roulement, y compris les ressources qui vous permettront de vous préparer pour le prochain changement, sont disponibles sur **https://icann.org/kskroll**.

Vous pouvez également envoyer un courrier électronique à **globalsupport@icann.org** en mettant « roulement de la KSK » dans la ligne objet du message, ou rejoindre la conversation sur Twitter en utilisant le hashtag #KeyRoll.

Conçu par le département des communications de l'ICANN | mars 2018