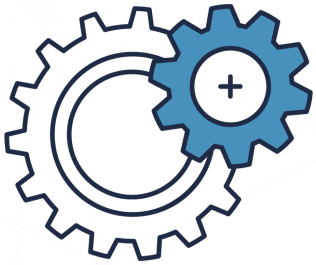
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

# COMMENT LES MISES À JOUR PROTÈGENT-ELLES VOS APPAREILS?

**MARS 2021** **ITSAP.10.096**

Afin de protéger vos appareils contre les cybermenaces, il importe de mettre à jour régulièrement les systèmes d'exploitation et les applications de votre appareil et d'installer les correctifs de sécurité. Les mises à jour et les correctifs permettent non seulement de corriger les bogues ou d'améliorer l'utilisation ou la performance des appareils, mais aussi de corriger les vulnérabilités de sécurité connues. Lorsqu'un fournisseur publie des correctifs de sécurité, suivez le processus de gestion des correctifs de votre organisation afin d'appliquer le correctif dans les plus brefs délais.

Une **vulnérabilité** est une lacune ou une faiblesse liée à la sécurité. Il peut y avoir des **vulnérabilités techniques** dans la conception, la mise en œuvre, l'exploitation ou la gestion d'un système, d'un appareil ou d'un service informatique.



## GESTION DES CORRECTIFS

La gestion des correctifs est le processus adopté par votre organisation pour obtenir, tester et installer les correctifs et les mises à niveau sur vos systèmes et vos appareils. Une bonne gestion des correctifs peut aussi vous aider à atténuer les risques associés aux vulnérabilités de sécurité. Vous pouvez en effet utiliser un logiciel de gestion automatisé des correctifs pour tenir à jour vos applications et logiciels. Vous trouverez ci-dessous d'importantes mesures de gestion des correctifs.

### TROUVER LE CORRECTIF

Les fournisseurs peuvent utiliser différents moyens pour communiquer les vulnérabilités et les correctifs. Certains fournisseurs publient des bulletins regroupés qui contiennent aussi les instructions recommandées sur le déploiement.

Le Centre pour la cybersécurité publie également des alertes et des bulletins sur les vulnérabilités qui touchent les infrastructures essentielles du Canada.

### TESTER LE CORRECTIF

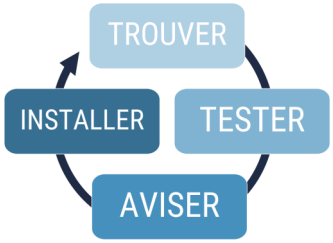
Vous devez tester le correctif avant de l'appliquer afin de confirmer qu'il est compatible avec votre environnement et logiciel existant. Vous devez aussi vérifier si des exigences additionnelles doivent être remplies pour que le correctif s'installe et fonctionne correctement.

### AVISER LES PERSONNES CONCERNÉES

Avisez toutes les personnes concernées que le correctif est disponible. Indiquez clairement les instructions à suivre pour appliquer le correctif et les délais connexes.

### INSTALLER LE CORRECTIF

Appliquez les correctifs de sécurité dès que possible afin de protéger vos appareils. Il est important de noter que l'installation du correctif peut perturber la fonctionnalité de l'appareil ou interrompre les programmes. Afin d'éviter toute interruption, planifiez les mises à jour et l'application des correctifs après les heures normales de travail.




En ce qui concerne les **appareils personnels**, il est recommandé d'activer les fonctions de mise à jour automatisées comme mesure de gestion des correctifs. Les correctifs appliqués automatiquement ne sont pas testés, mais vous réduisez quand même les risques de compromission puisqu'ils sont appliqués sur votre appareil dès qu'ils sont publiés.

**SÉRIE SENSIBILISATION**

## RISQUES ASSOCIÉS AUX CORRECTIFS

Nous vous recommandons d'installer les correctifs et les mises à jour pour sécuriser vos systèmes et vos appareils et en assurer le bon fonctionnement. Cependant, les correctifs peuvent perturber les fonctions opérationnelles des façons suivantes :

- Un correctif peut perturber les fonctions d'autres applications ou interrompre des programmes.
- Il est possible que vous deviez redémarrer les appareils, ce qui pourrait donner lieu à une perte de données.
- L'installation des correctifs pourrait faire ressortir d'autres lacunes du programme, y compris d'autres défauts de sécurité.

Pour réduire le risque d'interruption ou de perte de données, il convient d'analyser et de tester les correctifs avant de les installer dans votre environnement.

## AUTRES CONSIDÉRATIONS

### APPAREILS NON PRIS EN CHARGE

Nous recommandons de remplacer les systèmes et les appareils qui ne sont plus pris en charge, c'est-à-dire les systèmes et appareils pour lesquels le fabricant n'offre plus de soutien logiciel et ne diffuse plus de correctifs ni de mises à jour.

Les appareils hérités et non pris en charge sont plus sujets à des vulnérabilités qui ne seront jamais corrigées, ce qui accroît le niveau de risque assumé par votre organisation. De plus, les appareils hérités sont souvent des produits moins récents qui n'ont pas les capacités de sécurité actuelles.

### SOLUTIONS DE CONTOURNEMENT TEMPORAIRES

Si une mise à jour n'est pas encore disponible, vous pouvez utiliser une solution de rechange temporaire pour contourner les problèmes. Les solutions de contournement sont publiées par le fabricant dans le but de désactiver ou de limiter l'accès aux services vulnérables.

L'équipe de service de TI de votre organisation devrait assurer le suivi des solutions de contournement temporaires afin de veiller à ce que les correctifs soient téléchargés de manière à se superposer et à se prendre en charge mutuellement (plutôt que de se chevaucher). Les solutions de contournement ne sont pas permanentes. Il convient d'appliquer le correctif dès qu'il est disponible et de supprimer par la suite la solution de contournement.

## RISQUES ASSOCIÉS À LA NON-APPLICATION DES CORRECTIFS

Le fait d'ignorer ou de reporter l'installation des mises à jour ou des correctifs peut causer des problèmes liés à la performance et à la facilité d'utilisation des appareils, comme des applications qui ne répondent pas, des fonctionnalités non accessibles et des systèmes lents.

De plus, les auteurs de menace pourraient profiter des systèmes et des appareils non corrigés pour exploiter des vulnérabilités et infecter les appareils avec des maliciels ou accéder à de l'information.

### FOURNISSEURS DE SERVICES

Si vous avez confié vos services de TI à un fournisseur de services gérés ou à un fournisseur de services infonuagiques, votre fournisseur pourrait être responsable de la mise à jour des systèmes et de l'application des correctifs. Il convient de passer en revue votre contrat de service pour connaître les rôles et les responsabilités liées à la gestion des correctifs.

Même si vous utilisez un fournisseur de services, il vous revient d'installer les mises à jour et les correctifs sur les périphériques ou les systèmes et appareils qui ne font pas partie de votre contrat.

## LES QUATRE CONSEILS LES PLUS IMPORTANTS

1. Appliquez les correctifs pour assurer le fonctionnement ininterrompu et la sécurisation des appareils.
2. Envisagez l'utilisation d'un système de gestion des correctifs pour tenir à jour les appareils et les applications.
3. Analysez et testez les correctifs avant de les installer.
4. Utilisez des appareils pris en charge par le fabricant.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.