Application des mises à jour sur les dispositifs

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Février 2024 | ITSAP.10.096

La mise à jour des logiciels rectifie les vulnérabilités et protège les dispositifs. Les fournisseurs publient des correctifs pour corriger les bogues, résoudre les vulnérabilités et améliorer l'utilisabilité ou les performances. Il convient de noter que tous les correctifs sont des mises à jour, mais que les mises à jour ne constituent pas forcément des correctifs. Par exemple, une mise à jour peut être diffusée pour simplement mettre à niveau certaines fonctions logicielles, alors qu'un correctif servira essentiellement à combler une lacune particulière qui, autrement, vous exposerait, vous et votre organisation, à un risque accru de compromissions de données. Lorsqu'un fournisseur publie un correctif visant à combler une lacune de sécurité, votre organisme devrait prendre les dispositions nécessaires pour appliquer ce correctif dans les plus brefs délais.

Types de correctifs

- Correctif de bogue : Règle les problèmes liés aux fonctionnalités des logiciels, comme une erreur qui amène un dispositif à réagir de façon inattendue.
- Correctif de sécurité : Rectifie les vulnérabilités dans le but de protéger le système contre les menaces, comme un maliciel qui infecte les dispositifs suivant l'exploitation de vulnérabilités.
- Mise à jour des fonctions : Ajoute de nouvelles fonctions à un logiciel déjà installé, comme une amélioration des performances ou de la rapidité de traitement d'une application.

Gestion des correctifs

La gestion des correctifs consiste en une stratégie et un processus suivant lesquels un organisme peut acquérir, tester et installer des correctifs sur ses systèmes et ses dispositifs. Il est possible d'automatiser la gestion des correctifs, ce qui garantit la prompte mise à jour des applications et des logiciels.

Le processus de gestion des correctifs comprend les mesures suivantes :

surveiller la diffusion de nouveaux correctifs pour les appareils que vous utilisez; → tester les correctifs (si possible) pour s'assurer qu'ils sont compatibles avec l'environnement et les logiciels visés; → examiner les exigences additionnelles qui pourraient s'appliquer pour que les correctifs puissent être installés et fonctionner normalement; → envoyer des notifications lorsque des correctifs sont publiés; → installer les correctifs; → confirmer que les correctifs ont bien été appliqués.

Dans le cas des appareils personnels, il est recommandé de configurer la fonction de mise à jour automatique en guise de mesure de gestion des correctifs. Certes, les fonctions de mise à jour automatisées ne testent pas les correctifs, mais elles optimisent sans délai le niveau de sécurisation des dispositifs en appliquant les mesures requises dès qu'elles sont accessibles.

Solutions de contournement

Si une mise à jour n'est pas encore disponible, vous pouvez utiliser une solution de contournement pour contourner les problèmes. Les solutions de contournement sont diffusées par le fabricant dans le but de désactiver ou de limiter les accès aux services vulnérables. L'équipe des services informatiques de votre organisation devrait assurer le suivi des solutions de contournement 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).

Il faut donc se rappeler que 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.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Février 2024 | ITSAP.10.096

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 accroître le niveau de risque encouru par l'organisme. Voici certains de ces risques :

- le système ralentit considérablement ou plante en cours d'utilisation;
- certaines applications ne répondent plus;
- les vulnérabilités sont exploitées de façon à favoriser l'infection des dispositifs par des maliciels;
- les auteures et auteurs malveillants peuvent avoir accès à votre information sensible, la voler ou la chiffrer, ou nuire au bon fonctionnement de votre appareil;
- certaines fonctionnalités ou applications ne sont plus accessibles.

Risques associés à l'application des correctifs

Il est fortement recommandé d'installer les correctifs et les mises à jour dès que possible pour garantir le bon fonctionnement et la sécurité de vos appareils et de vos systèmes. Il faut savoir que l'installation des correctifs et des mises à jour comporte certains risques. Par exemple :

- l'installation de correctifs peut perturber les fonctions d'autres applications;
- le redémarrage des appareils qui viennent d'être mis à jour peut interrompre d'autres programmes, ce qui pourrait donner lieu à des pertes de données ou à des interruptions de service;
- l'installation des correctifs pourrait faire ressortir d'autres lacunes du programme, dont d'autres failles de sécurité.

Pour éviter ces risques, il convient de sauvegarder vos données, puis d'examiner et de tester les correctifs avant de les installer. Pour en apprendre davantage, reportez-vous à la publication *Sauvegarder et récupérer vos données* (ITSAP.40.002).

On comprend que le téléchargement de correctifs peut perturber certaines fonctions des dispositifs, comme le redémarrage prévu à une certaine date et heure. Il est toutefois recommandé de mettre à jour les correctifs de sécurité aussi régulièrement que possible, de façon à assurer la sécurisation des dispositifs.

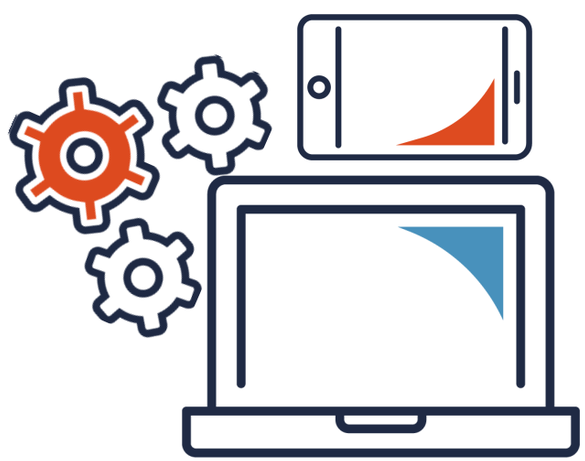
L'application de correctifs devrait être considérée comme un processus continu en ce qui a trait aux activités informatiques de votre organisation.

Appareils non pris en charge

Les dispositifs patrimoniaux et qui ne sont pas pris en charge sont ceux pour lesquels le fabricant ne diffuse plus de correctifs ni de mises à jour. Ils sont susceptibles de présenter des vulnérabilités qui ne seront vraisemblablement jamais corrigées, ce qui accroît le niveau de risque encouru par votre organisation. Nous recommandons donc de remplacer les systèmes pour lesquels le fabricant ne diffusera plus de correctifs ni de mises à jour.

Les conseils les plus importants

- L'application des correctifs favorise le fonctionnement ininterrompu et la sécurisation des dispositifs.
- Le recours à un système de gestion des correctifs permet à l'organisation de travailler avec des applications et des dispositifs qui sont toujours à jour.
- L'examen et la mise à l'essai des correctifs constituent des étapes importantes du processus de gestion des correctifs et doivent précéder l'étape de l'installation.
- L'utilisation de dispositifs qui sont pris en charge par leur fabricant garantit que les systèmes reçoivent, en temps opportun, les correctifs et les mises à jour nécessaires.



Centre de la sécurité des télécommunications
Communications Security Establishment

Canada