CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SI-02

Correction des défauts

Juill. 2026

Votre gouvernement

Québec

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-02 — Correction des défauts (-F-) (Obligatoire)

Énoncés :

a. Identifier, signaler et corriger les défauts du système
b. Tester les mises à jour logicielles et micrologicielles visant la correction des défauts pour en vérifier l'efficacité et les répercussions potentielles sur les systèmes avant leur application
c. Installer les mises à jour de sécurité appropriées des logiciels et des micrologiciels dans une période de [Affectation : période définie par l'organisation] suivant la date de publication des mises à jour
d. Intégrer la correction des défauts au processus de gestion des configurations de l'organisation

Paramètres :

c. délais prescrits par le processus de gestion des menaces, vulnérabilités et incidents (GMVI)
aaQC. systèmes d'exploitation et logiciels; serveurs, postes de travail (incluant les postes gérés se situant hors du réseau de confiance), appareils mobiles et équipements réseau

Responsable : Partagée

Date limite de mise en oeuvre : 2021-06-30

Discussion :

La nécessité de corriger les défauts du système s'applique à tous les types de logiciels et de micrologiciels. Les organisations identifient les systèmes touchés par les défauts logiciels, y compris les possibles vulnérabilités résultant de ces défauts, et font rapport de cette information au personnel responsable de la sécurité et de la protection de la vie privée de l'information. Les organisations envisagent d'établir un environnement contrôlé d'application de correctifs pour les systèmes essentiels à la mission. Les mises à jour liées à la sécurité incluent les correctifs, les ensembles de modifications provisoires et les signatures de code malveillant. Les organisations corrigent également le plus rapidement possible les défauts relevés durant les évaluations, la surveillance permanente, les activités liées aux interventions en cas d'incident ou le traitement des erreurs du système. En intégrant la correction des défauts aux processus de gestion des configurations, il est possible d'assurer le suivi et la vérification des mesures correctrices requises. Le délai défini par l'organisation pour les mises à jour de sécurité logicielles et micrologicielles peut varier en fonction de divers facteurs de risque, notamment, la catégorie de sécurité du système, la criticité de la mise à jour (c'est-à-dire la gravité de la vulnérabilité liée au défaut découvert), la tolérance au risque de l'organisation, la mission prise en charge par le système ou l'environnement de menace. Certains types de correctifs peuvent nécessiter plus de mises à l'essai que d'autres. Les organisations doivent déterminer le type de mises à l'essai nécessaires pour le type précis de correction des défauts considérés et le type de changements dont la configuration doit être gérée. La mise à l'essai de la correction des défauts permet d'analyser l'efficacité des mesures prises pour corriger des problèmes de sécurité et les effets secondaires possibles sur la fonctionnalité des systèmes et des composants de systèmes, leurs performances et leur exploitation. Au moment de mettre en oeuvre des activités d'atténuation, les organisations considèrent l'ordre et l'horaire des mises à jour pour valider leur exécution appropriée dans l'environnement du système et soutenir les besoins du système et du composant en matière de disponibilité (c'est-à-dire la mise en oeuvre d'une stratégie de déploiement progressive). Les organisations s'assurent que les mises à jour logicielles et micrologicielles proviennent de sources autorisées avant leur téléchargement. Dans le cadre de ces décisions de mise à l'essai, l'organisation détermine si les mises à jour logicielles ou micrologicielles proviennent de sources autorisées ayant les signatures numériques appropriées.