Communications Security Establishment | Centre de la sécurité des télécommunications

Correction des systèmes d'exploitation et des applications

Bulletin de sécurité des TI à l'intention du gouvernement du Canada

ITSB-96 **Dernière mise à jour : mars 2015**

1 Introduction

La correction des systèmes d'exploitation et des applications est l'une des 10 mesures de sécurité des TI les mieux à même de protéger les réseaux Internet et l'information du gouvernement du Canada (ITSB-89, version 3). La mise en œuvre simultanée de ces 10 mesures de sécurité permettrait de prévenir la grande majorité des intrusions auxquelles le CST doit réagir actuellement.

L'application de correctifs aux systèmes d'exploitation, aux applications et aux dispositifs est primordiale lorsqu'il s'agit d'assurer la sécurité des systèmes. Le présent document propose des conseils en matière d'évaluation des vulnérabilités connues et des correctifs, qui permettront d'estimer les risques pour l'organisme, d'établir l'ordre de priorité dans lequel les correctifs doivent être déployés et de déterminer les modalités de déploiement desdits correctifs.

2 Pourquoi les correctifs?

Le cas échéant, les fournisseurs de logiciels découvrent et dévoilent les vulnérabilités de leurs produits, puis ils publient des correctifs visant à éliminer lesdites vulnérabilités. Or, par la même occasion, ils informent les adversaires des vulnérabilités décelées. Par ailleurs, on constate regrettablement que de nombreux organismes n'installent pas les correctifs immédiatement après leur publication. Cette omission permet aux adversaires d'analyser les faiblesses du réseau et d'élaborer des moyens de l'exploiter, et ce, jusqu'à ce que l'organisme déploie les correctifs appropriés.

> Il importe d'appliquer rapidement les correctifs, puisque les exploits publics se multiplient sitôt que les correctifs sont diffusés.
>
> En à peine quelques heures, des adversaires sont déjà en mesure d'utiliser des techniques de rétroingénierie dans l'intention de déjouer les correctifs.

3 Évaluation des vulnérabilités de sécurité et des correctifs

Le personnel dispose de nombreuses sources d'information lui permettant d'évaluer les risques liés à une vulnérabilité ainsi que les correctifs correspondants dans un contexte semblable à l'environnement de technologies de l'information (TI) où il évolue. En l'occurrence, l'avis du fournisseur concernant le correctif constitue l'une des principales sources d'information.

L'information du fournisseur sur la vulnérabilité et le correctif comprend habituellement ce qui suit :

- la liste des produits et versions touchés;
- des détails techniques sur la vulnérabilité, notamment un aperçu de la méthode d'exploitation;
- les conséquences types de son exploitation (p. ex. exécution de code, divulgation d'information, déni de service, etc.);
- l'état actuel de l'exploitation (c.-à-d. le fait d'établir si la vulnérabilité est déjà exploitée ou non);
- les solutions de contournement temporaires, le cas échéant;
- l'indice de gravité de la vulnérabilité en fonction des facteurs énoncés précédemment.

Chaque fournisseur a recours à sa propre méthode pour communiquer la gravité d'une vulnérabilité. L'échelle de gravité peut être fondée sur une norme, comme le système de notation CVSS (pour *Common Vulnerability Scoring System*), ou encore sur des catégories définies par le fournisseur, par exemple « Critique » ou « Important ».

Quel que soit le système utilisé par le fournisseur, ces échelles de gravité peuvent aider le personnel des TI à mener rapidement un premier diagnostic sur les risques d'exploitation d'une vulnérabilité dans son environnement.

En plus des détails sur les vulnérabilités et sur les correctifs, certains fournisseurs publient des bulletins réguliers comportant des instructions concernant les déploiements recommandés.

4 Évaluation des risques relatifs à une vulnérabilité et au correctif

Le personnel du ministère doit analyser l'information sur la vulnérabilité et sur le correctif avant de mener une évaluation des risques. L'évaluation des risques permet au ministère d'établir correctement le niveau de gravité d'une vulnérabilité dans le contexte de son propre environnement.

Pendant l'évaluation des risques, il importe de prendre en compte les facteurs suivants :

- répercussions sur les actifs de grande valeur ou à exposition élevée – risques accrus;
- répercussions sur les actifs ayant déjà fait l'objet d'attaques – risques accrus;
- mesures d'atténuation en place (actuellement ou prochainement) – pour tous les biens touchés – risques atténués;
- faible niveau de risque pour les actifs touchés – risques atténués.

Exemples d'évaluation des risques liés à une vulnérabilité/un correctif

- **Risque extrême**
  - la vulnérabilité permet l'exécution de code à distance;
  - des systèmes ou de l'information essentiels aux activités sont touchés;
  - des exploits existent et sont utilisés;
  - le système est connecté à Internet, mais aucune mesure d'atténuation n'est en place.
- **Risque élevé**
  - la vulnérabilité permet l'exécution de code à distance;
  - des systèmes ou de l'information essentiels aux activités sont touchés;
  - des exploits existent et sont utilisés;
  - le système est dans une enclave protégée par des contrôles d'accès robustes.
- **Risque moyen**
  - la vulnérabilité permet à un attaquant de se faire passer pour un utilisateur légitime au moyen d'un accès à distance;
  - le système est exposé à des utilisateurs non authentifiés;
  - le système nécessite une authentification à deux facteurs, et les ouvertures de session à distance des administrateurs sont désactivées.
- **Risque faible**
  - la vulnérabilité peut être exploitée seulement si un utilisateur authentifié exécute une action malveillante, comme une injection SQL;
  - le système touché contient seulement de l'information publique ou peu sensible;
  - les mesures d'atténuation en place rendent toute tentative d'exploitation peu probable ou très difficile.

Exemples simplifiés d'évaluation de risques associés au correctif :

Service	Vulnérabilité	Mesures de sécurité en place	Niveau de risque
Ministère A	Exécution de code à distance dans Microsoft Office	Aucune	**Extrême**
Ministère B		Filtrage efficace du contenu des courriels ET filtrage efficace du contenu des courriels	**Élevé**
Ministère C		Filtrage efficace du contenu des courriels ET liste blanche des applications ET filtrage efficace du contenu des courriels	**Moyen**

5 Échéanciers de déploiement des correctifs

Une fois que le fournisseur a diffusé un correctif et que le personnel du ministère a établi la gravité de la vulnérabilité et l'applicabilité du correctif, ce dernier doit être déployé plus ou moins rapidement selon le niveau de risque d'exploitation de ladite vulnérabilité.

Pour veiller à ce que les ressources TI soient employées efficacement, il faut d'abord se concentrer sur les problèmes les plus importants.

Le CST recommande donc de suivre les échéanciers de déploiement suivants pour les divers niveaux de risques liés aux vulnérabilités/aux correctifs :

- **Extrême :** dans les 48 heures;
- **Élevé :** dans les deux semaines;
- **Moyen :** à la prochaine mise à jour ou dans les trois mois;
- **Faible :** à la prochaine mise à jour ou dans les douze mois.

6 Essai des correctifs

Le ministère doit établir quel risque est le plus important : la non-correction des vulnérabilités, ce qui expose le ministère à un risque de compromission, ou encore le déploiement d'un correctif que le ministère n'a pas testé de manière exhaustive. De nombreux fournisseurs, y compris Microsoft, mènent des tests exhaustifs sur tous leurs correctifs avant leur diffusion, et ce, en fonction d'un large éventail d'environnements, d'applications et de conditions.

Le ministère peut commencer par déployer un correctif auprès d'un groupe de test composé d'employés de toutes les unités opérationnelles du ministère (p. ex. RH, Finances, Opérations). Si aucun défaut n'est signalé dans les 48 heures, le ministère peut procéder au déploiement global du correctif en question. Il peut également envisager de mettre en œuvre des systèmes permettant d'automatiser l'essai des correctifs dans son environnement.

7 Application d'un correctif

L'application des correctifs peut se faire au moyen d'un système de gestion des correctifs. Ce type de système facilite la réception, l'essai et l'installation des correctifs, ce qui permet d'optimiser la protection de l'environnement d'exploitation.

Voici quelques pratiques couramment utilisées :

- Avant d'installer de nouveaux correctifs, les administrateurs de systèmes doivent passer en revue toute l'information contextuelle liée auxdits correctifs, y compris les exigences d'installation. Des recherches additionnelles peuvent s'avérer nécessaires pour établir, par exemple, s'il existe des problèmes potentiels relatifs à l'installation des correctifs.
- Après l'application des correctifs, il faut procéder à une vérification visant à mesurer leur taux de réussite et à confirmer leur efficacité.
- Il est recommandé de se tenir au courant des nouveautés concernant les correctifs, les systèmes d'exploitation de réseau et les mises à jour que produisent les fournisseurs. Les administrateurs de systèmes connaîtront ainsi les nouvelles vulnérabilités et pourront appliquer les correctifs nécessaires dans les plus brefs délais.

8 Solutions de contournement temporaires

Une solution de contournement temporaire est parfois la seule protection efficace qui s'offre à l'administrateur, lorsque le fournisseur n'a pas encore diffusé de correctif. Le fournisseur présente habituellement ces solutions de contournements au moment où une vulnérabilité est annoncée ou peu de temps après.

Voici quelques exemples de solutions de contournement temporaires : désactiver la fonction vulnérable du logiciel ou du dispositif; restreindre ou bloquer l'accès au service vulnérable au moyen de coupe-feux ou d'autres contrôles d'accès.

Comme pour l'application de correctifs, le risque évalué dictera si le ministère doit appliquer ou ne pas appliquer une solution de contournement temporaire.

9 Renseignements additionnels

La liste intégrale des 10 mesures de sécurité des TI les mieux aptes à protéger les réseaux Internet et l'information du gouvernement du Canada ainsi que des conseils additionnels se trouvent à l'adresse suivante : http://www.cse-cst.gc.ca/fr/group-groupe/conseil-directives-matiere-sti. Le document Microsoft's Security Update Guide présente le processus de mise à jour de sécurité de Microsoft et fournit des conseils sur la façon dont le personnel des TI peut analyser les risques liés aux vulnérabilités et procéder à l'installation des mises à jour.

10 Coordonnées et assistance

Services à la clientèle de la STI
Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca