Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Juillet 2013

Atténuation des vulnérabilités de Java

Conseils à l'intention du gouvernement du Canada

ITSB-98

Introduction

Java est un langage de programmation et une plateforme informatique servant à de nombreux processus opérationnels et systèmes autorisés. Sa clientèle établie s'élève à près d'un milliard d'utilisateurs. Au cours de la dernière année, des cyberintrus ont découvert et exploité bon nombre des vulnérabilités de Java. Certains exploits pourraient compromettre, sans avertissement, la sécurité de l'information sur le réseau du ministère. Le délai entre la découverte d'une vulnérabilité et la conception et mise en œuvre d'un correctif facilite l'exploitation de la vulnérabilité en question par les cyberintrus. Or, le réseau d'un ministère demeure vulnérable aux attaques pendant une période prolongée.

Auditoire cible

Le présent bulletin est destiné aux praticiens de la sécurité informatique responsables des activités de gestion des risques liés à la sécurité des technologies de l'information (STI). Il est structuré de manière à être utilisé dans le cadre des activités de gestion de la STI définies dans la publication du CSTC suivante : *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33).

Vulnérabilité

En janvier 2013, on a rendu publique[1] la reconnaissance d'un exploit d'une vulnérabilité du logiciel Java d'Oracle. La vulnérabilité a été décelée dans Java Development Kit (JDK) et Java Runtime Environment (JRE), deux produits déployés sur la plupart des ordinateurs personnels et d'entreprises. Cet exploit de type « jour zéro » incitait les utilisateurs à parcourir un site Web malveillant au moyen de leur navigateur Java. Dès que le navigateur se connectait au site infecté, un programme Java malveillant contournant les vérifications de sécurité était exécuté, permettant du coup à un auteur de menace à distance d'obtenir tous les accès administratifs au système de l'utilisateur. Même si un correctif a rapidement été diffusé, un autre exploit de type « jour zéro » a rapidement été créé pour le contourner.

Diverses versions de Java peuvent être utilisées et exploitées de différentes manières, puisqu'il est possible d'accéder à Java au moyen d'un navigateur Web ou d'un système central. Étant donné le nombre de navigateurs Java, il va sans dire que la surface d'attaque est vaste. Les ministères devraient d'ailleurs réviser leur évaluation des menaces et des risques en matière de STI afin de tenir compte des vulnérabilités actuelles liées à Java et d'inclure une réévaluation des risques résiduels de compromission du contenu de leur réseau.

Incidence sur le gouvernement du Canada (GC)

La plateforme Java est installée sur des milliers de systèmes du GC. Des ministères dépendent des applications Java, qu'elles soient en lignes ou au niveau du système central, pour exécuter des processus opérationnels valides. Dans la majorité des cas, les systèmes qui utilisent les applications Java font partie de réseaux avec accès à Internet. Cette situation pose un problème si Java est connecté au navigateur par défaut et que l'utilisateur visite un site Web malveillant. L'ordinateur peut alors être exploité grâce aux vulnérabilités du module Java et exposer le contenu du réseau du ministère à des accès non autorisés.

---

[1] Plus précisément, l'exploit CVE-2013-0422 ciblait la mise à jour 10 (et les précédentes) de Java 7; les versions antérieures de Java n'étaient pas touchées.

Mesures d'atténuation recommandées

On recommande les options suivantes pour atténuer les exploits Java :

1. Installation des correctifs

Selon *Les 35 mesures d'atténuation les plus efficaces du CSTC* (ITSB-89A), l'application de correctifs est la mesure d'atténuation no 2. Les administrateurs de systèmes doivent veiller à l'application des correctifs les plus récents aux produits Java.

2. Désinstallation de Java

Si les activités opérationnelles normales du ministère n'exigent pas l'utilisation de Java, l'application devrait être désinstallée. Cette mesure protégera les biens de TI contre les exploits actuels et futurs.

3. Restriction de la navigation Java à un environnement virtuel

En limitant la navigation Java à un système d'exploitation virtuel, on peut faire en sorte que toute corruption de l'environnement résultant d'un exploit Java ait peu de répercussions sur le système physique, et ce, particulièrement si l'environnement virtuel est non persistant et qu'il rétablit sa configuration sécurisée après l'utilisation ou le redémarrage.

4. Désactivation du plugiciel Java

Le plugiciel Java peut être désactivé dans tous les navigateurs si Java n'est pas requis pour les processus ministériels essentiels.

5. Désactivation de Java dans le navigateur par défaut

Cette option est utilisée lorsqu'un ministère doit régulièrement utiliser un programme Java en ligne et exige que les utilisateurs utilisent deux navigateurs; à savoir un pour une navigation limitée sur Internet avec Java, et un autre pour toutes les autres utilisations d'Internet. Java doit être désactivé dans le navigateur par défaut, de manière à ne pas être facilement accessible si le navigateur est lancé par un programme malveillant. Si l'utilisation de Java est nécessaire, les utilisateurs peuvent alors utiliser le second navigateur, sur lequel Java est activé. Il faut noter que cette option n'est viable que si les utilisateurs respectent strictement les lignes directrices d'utilisation des navigateurs, ou si la navigation Java est limitée à des sites Web sécuritaires.

6. Restriction de l'accès à Java au niveau du coupe-feu

Cette option permet au ministère de continuer à utiliser Java à l'interne ainsi que sur certains sites Web et d'atténuer les risques liés aux vulnérabilités en limitant l'accès à Java pour les sites interdits. La restriction de l'accès requiert l'utilisation de règles au niveau des serveurs mandataires dans le but de contrôler l'utilisation de Java, par exemple :

- la création d'une liste blanche[2] des sites Web essentiels qui utilisent Java et le blocage de tous les autres;
- le filtrage des demandes contenant des en-têtes d'agent utilisateur Java pour permettre l'utilisation de Java sur le réseau du ministère tout en bloquant les autres demandes;
- le blocage du trafic sortant dont les extensions sont les suivantes : jar, cla, class, jnlp, jardiff et java.

[2] Une « liste blanche » est un registre des sites Web de confiance pour lesquels on permet l'utilisation de Java.

Sommaire

Même si Java est un outil de travail utile, il est devenu le centre d'intérêt des cyberintrus qui continuent d'exposer et d'exploiter ses vulnérabilités. Ces vulnérabilités peuvent nuire à la sécurité des réseaux du GC.

On recommande aux ministères d'éviter de dépendre de produits qui ne fonctionnent pas sans Java, tout particulièrement si ces produits exigent l'installation de Java sur un poste de travail qui sera utilisé pour naviguer sur Internet et pour la messagerie électronique. Si cela s’avère possible, la mesure d'atténuation à privilégier est la suppression de Java du réseau d'un ministère.

Autres renseignements

Prière de communiquer avec les Services à la clientèle au itsclientservices@cse-cst.gc.ca pour obtenir plus de conseils sur la sécurité des TI.