Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 09 août 2000
N° CERTA-2000-AVI-026

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Netscape avec Java

Gestion du document

Référence	CERTA-2000-AVI-026
Titre	Vulnérabilité de Netscape avec Java
Date de la première version	09 août 2000
Date de la dernière version	–
Source(s)	Avis du CIAC Réseau de confiance
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Accès en lecture aux données de l'utilisateur depuis un poste distant.

2 Systèmes affectés

Netscape Navigator toutes versions et Communicator 4.74 et inférieures si java est activé. Vulnérabilité indépendante du système d'exploitation.

3 Résumé

Une vulnérabilité de la machine virtuelle java (*java Virtual Machine*) a été découverte sur Netscape Navigator et Communicator. Elle permet à un serveur web hostile de démarrer un processus serveur à l'insu de l'utilisateur qui navigue sur ce site. Ce processus permet à n'importe quel navigateur web de lire toutes les données locales accessibles par l'utilisateur connecté.

4 Description

Un administrateur mal intentionné ayant déposé sur son site web une applet java peut lire le contenu du disque des utilisateurs possédant Netscape Navigator ou Communicator et ayant activé java. Ceci n'est possible que si l'utilisateur se connecte au site hostile et si java est activé.

L'applet java exécutée par le client parcourant le site hostile le transforme alors en serveur web rendant toutes les données auxquelles l'utilisateur à accès, y compris celles situées sur des répertoires ou disques réseaux, visibles par internet.

De nombreuses exploitations ont déjà été diffusées sur internet.

Il n'est pas exclus que des adaptations soient développées sous tout navigateur, et avec toutes sortes de langages, notamment ActiveX pour Internet Explorer ou Visual Basic, ou étendu aux mails aux formats HTML.

5 Contournement provisoire

Tout site doit avoir un garde-barrière, la configuration de ce garde-barrière doit interdire les connexions vers les machines protégées. En d'autre terme les client du site protégé ne peuvent pas être des serveurs vers internet grâce aux règles du garde-barrière.

Il est donc important de ne pas naviguer depuis un serveur, car il n'est pas protégé par le garde-barrière.

Le port d'écoute du serveur peut être déterminé par l'administrateur mal intentionné, il n'est donc pas prévisible.

Cette mesure ne protègera pas contre une attaque de l'intérieur.

6 Solution

Il n'y a pas de correctif actuellement disponible.

Désactiver Java du navigateur web.

Pour prévenir toute évolution, désactiver aussi ActiveX des navigateurs Internet Explorer.

7 Documentation

- avis K-063 du CIAC :
  http://www.ciac.org/ciac/bulletins/k-063.shtml
- Site ou la vulnérabilité de Java dans Netscape est décrite, et où on peut trouver un exemple d'exploitation.
  http://www.brumleve.com/BrownOrifice/
  Nota : Cet exemple, et les multiples autres déjà présents sur le web peuvent être modifiés pour un usage encore plus malfaisant

Gestion détaillée du document

09 août 2000 version initiale.