Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 avril 2003
N° CERTA-2003-AVI-081

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Microsoft Internet Explorer

Gestion du document

Référence	CERTA-2003-AVI-081
Titre	Vulnérabilités de Microsoft Internet Explorer
Date de la première version	28 avril 2003
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS03-015
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

- Exécution de code arbitraire ;
- divulgation d'informations.

2 Systèmes affectés

- Microsoft Internet Explorer 5.01 ;
- Microsoft Internet Explorer 5.5 ;
- Microsoft Internet Explorer 6.0.

3 Résumé

Quatre vulnérabilités de Microsoft Internet Explorer ont été découvertes et peuvent être exploitées par le biais d'un site web ou d'un mél au format HTML habilement contruit.

4 Description

– Première vulnérabilité (CVE CAN-2003-0113) : un débordement de mémoire dans la bibliothèque *URLMON.DLL* permet à un utilisateur mal intentionné d'exécuter du code arbitraire.

– Deuxième vulnérabilité (CVE CAN-2003-0114) : le programme de contrôle de téléchargement de fichiers (*File Upload Control*) est vulnérable et permet à un utilisateur mal intentionné de récupérer n'importe quel fichier situé sur le disque dur de la victime.

– Troisième vulnérabilité (CVE CAN-2003-0115) : Internet Explorer ne gère pas correctement les liens hypertextes (URL) qui invoquent un module d'une application tierce. Il est alors possible d'exécuter du script sur la machine vulnérable dans la zone de sécurité locale.

– Quatrième vulnérabilité (CVE CAN-2003-0116) : un paramètre des feuilles de style (*Cascading Style Sheet*) utilisées pour les boîtes de dialogue (*Modal Dialog*) n'est pas vérifié et permet à un utilisateur mal intentionné d'exécuter un script sur l'ordinateur de la victime.

5 Solution

Appliquer le correctif fourni par Microsoft :
http://www.microsoft.com/windows/ie/downloads/critical/813489.asp

6 Documentation

– Avis de sécurité Microsoft MS03-015 :
http://www.microsoft.com/technet/security/bulletin/MS03-015.asp

– Références CVE CAN-2003-0113 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0113

– Références CVE CAN-2003-0114 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0114

– Références CVE CAN-2003-0115 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0115

– Références CVE CAN-2003-0116 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0116

Gestion détaillée du document

28 avril 2003 version initiale.