Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2005
N° CERTA-2005-AVI-060

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans Internet Explorer

Gestion du document

Référence	CERTA-2005-AVI-060
Titre	Multiples Vulnérabilités dans Internet Explorer
Date de la première version	10 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-014 du 08 février 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

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

1 Risque

- Exécution de code arbitraire à distance ;
- élévation des privilèges ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 3 & 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP 64-bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 pour systèmes Itanium ;
- Microsoft Windows 98 & 98 Second Edition ;
- Microsoft Windows Millennium Edition.

3 Résumé

De nombreuses vulnérabilités découvertes dans Microsoft Internet Explorer permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, d'élever ses privilèges ou de porter atteinte à la confidentialité des données présentes sur le système vulnérable.

4 Description

L'application Microsoft Internet Explorer présente quatres vulnérabilités :

- La première vulnérabilité de type "`drag-and-drop`", qui signifie "`glisser et déposer`", permet à une personne malveillante à l'aide d'un site web malicieusement construit d'élever ses privilèges afin d'enregistrer un fichier malicieux sur le système vulnérable. L'exécution du fichier nécessite l'interaction de la victime (CAN-2005-0053) ;
- Une seconde vulnérabilité est dûe à un mauvais traitemente des adresses réticulaires (URL) par Internet Explorer, permettant à un individu mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de la victimes (CAN-2005-0054) ;
- La troisième vulnérabilité permet à une personne malveillante peut au moyen d'un d'une page web ou d'un mail malicieusement constitué, exécuter à distance un code arbitraire avec les privilèges de la victimes (CAN-2005-0055) ;
- La dernière vulnérabilité est de type `cross-domain`. Elle permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de la victime ou de porter atteinte à la confidentialité des données présentes sur le système vulnérable, par le biais d'une page web malicieusement construite (CAN-2005-0056).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS05-014 du 08 février 2005 :
  http://www.microsoft.com/technet/security/bulletin/MS05-014.mspx
- Référence CVE CAN-2005-0053 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053
- Référence CVE CAN-2005-0054 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0054
- Référence CVE CAN-2005-0055 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0055
- Référence CVE CAN-2005-0056 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0056

Gestion détaillée du document

10 février 2005 version initiale.