Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2004
N° CERTA-2004-AVI-241

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les fichiers d'aide HTML de Microsoft

Gestion du document

Référence	CERTA-2004-AVI-241
Titre	Vulnérabilités dans les fichiers d'aide HTML de Microsoft
Date de la première version	15 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-023
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

- Contournement de la politique de sécurité ;
- Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 2, Service Pack 3 et Service Pack 4 ;
- Microsoft Windows XP et XP Service Pack 1 ;
- 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 64-Bit Edition ;
- Microsoft Windows 98 et 98 SE ;
- Microsoft Windows Millennium Edition ;
- Internet Explorer 6.0 Service Pack 1 installé sur Windows NT 4.0 SP6a.

3 Résumé

Deux vulnérabilités présentes dans les fonctions d'aide de Windows permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Deux vulnérabilités permettent à un utilisateur distant mal intentionné, par le biais d'une adresse réticulaire (URL) d'aide malicieusement constuite, d'exécuter du code arbitraire sur la machine cible. Si l'utilisateur est connecté en tant qu'administrateur, il est possible pour l'attaquant d'avoir les mêmes droits.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS04-023 du 13 juillet :
  http://www.microsoft.com/technet/security/bulletin/ms04-023.mspx
- Référence CVE CAN-2003-1041 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1041
- Référence CVE CAN-2004-0201 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0201

Gestion détaillée du document

15 juillet 2004 version initiale.