Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 juillet 2004
N° CERTA-2004-AVI-260

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Internet Explorer

Gestion du document

Référence	CERTA-2004-AVI-260
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	31 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-025
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 à distance.

2 Systèmes affectés

Ces vulnérabilités affectent les versions suivantes d'Internet Explorer :

- Internet Explorer 5.01 Service Pack 2, 3 et 4;
- Internet Explorer 5.5 Service Pack 2 ;
- Internet Explorer 6 ;
- Internet Explorer 6 Service Pack 1 ;
- Internet Explorer 6 Service Pack 1 (64-Bit Edition) ;
- Internet Explorer 6 pour Windows 2003 ;
- Internet Explorer 6 pour Windows 2003 (64-Bit Edition).

sur les plateformes :

- Microsoft Windows NT Workstation 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Service Pack 6a ;

- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 2, 3 et 4 ;
- Microsoft Windows XP et 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 ;
- Microsoft Windows 98 Second Edition (SE) ;
- Microsoft Windows Millennium Edition (Me).

3 Résumé

Trois vulnérabilités ont été découvertes dans Microsoft Internet Explorer permettant à un individu mal intentionné d'exécuter du code arbitraire à distance.

4 Description

- Une vulnérabilité présente dans la méthode de navigation d'Internet Explorer permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance dans la zone de sécurité `Local Machine Zone` avec les privilèges de l'utilisateur connecté, par l'intermédiaire d'un site malicieusement constitué (vulnérabilité CVE CAN-2004-0549) ;
- deux vulnérabilités sont présentes dans la méthode de traitement des images au format BMP (vulnérabilité CVE CAN-2004-0566) et au format GIF (vulnérabilité CVE CAN-2003-1048). Un utilisateur mal intentionné peut mettre à disposition un site web contenant des images malicieusement construites afin d'exécuter du code arbitraire sur la machine victime avec les privilèges de l'utilisateur connecté.

5 Solution

Se référer au bulletin de sécurité Microsoft afin d'obtenir la liste des correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS04-025 :
  http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx
- Référence CVE CAN-2004-0549 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0549
- Référence CVE CAN-2004-0566 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0566
- Référence CVE CAN-2003-1048 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1048

Gestion détaillée du document

31 juillet 2004 version initiale.