



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 juin 2005
N° CERTA-2005-AVI-218

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Internet Explorer

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-218>

Gestion du document

Référence	CERTA-2005-AVI-218
Titre	Vulnérabilités dans Internet Explorer
Date de la première version	15 juin 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-025 du 14 juin 2005
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

Les systèmes d'exploitation suivants sont affectés :

- Microsoft Windows 2000 Service Pack 3 et 4 ;
- Microsoft Windows XP Service Pack 1 et 2 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour systèmes Itanium ;
- Microsoft Windows Server 2003 Service Pack 1 pour systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows 98, Microsoft Windows 98 Seconde Edition et Microsoft Windows Millenium Edition.

Les logiciels suivants sont vulnérables :

- Internet Explorer 5.01 Service Pack 3 sur Microsoft Windows 2000 Service Pack 3 ;
- Internet Explorer 5.01 Service Pack 4 sur Microsoft Windows 2000 Service Pack 4 ;
- Internet Explorer 6 Service Pack 1 sur Microsoft Windows 2000 Service Pack 3 et 4 ou sur Microsoft Windows XP Service Pack 1 ;
- Internet Explorer 6 sur Microsoft Windows XP Service Pack 2 ;
- Internet Explorer 6 Service Pack 1 sur Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Internet Explorer 6 sur Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Internet Explorer 6 sur Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium), sur Microsoft Windows 2003 Server pour systèmes Itanium et sur Microsoft Windows 2003 Server Service Pack 1 pour systèmes Itanium ;
- Internet Explorer 6 sur Microsoft Windows 2003 Server x64 Edition et sur Microsoft Windows XP Professional x64 Edition ;
- Internet Explorer 5.5 Service Pack 2 sur Microsoft Windows Millenium Edition ;
- Internet Explorer 6 Service Pack 1 sur Microsoft Windows 98, Microsoft Windows 98 Seconde Edition, et sur Microsoft Windows Millenium Edition.

3 Résumé

Deux vulnérabilités découvertes dans le navigateur Internet Explorer permettent l'exécution de code arbitraire à distance.

4 Description

- Une vulnérabilité a été découverte dans le traitement des images au format PNG (Portable Network Graphics) par Internet Explorer. En incitant un internaute à visiter un site web ou à visualiser un mël contenant une image au format PNG malicieusement constituée, un utilisateur mal intentionné peut exécuter du code arbitraire à distance (référence CVE CAN-2005-1211) ;
- une vulnérabilité a été découverte dans le traitement des fichiers XML (eXtensible Markup Language). En incitant un internaute à visiter un site web ou à visualiser un mël malicieusement constitués, un utilisateur mal intentionné peut lire des données XML d'un autre domaine Internet Explorer (référence CVE CAN-2002-0648).

5 Solution

Appliquer le correctif de Microsoft (voir section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS05-025 du 14 juin 2005 :
<http://www.microsoft.com/technet/security/Bulletin/MS05-025.mspx>
- Référence CVE CAN-2005-1211 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1211>
- Référence CVE CAN-2002-0648 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0648>

Gestion détaillée du document

15 juin 2005 version initiale.