



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 août 2005
N° CERTA-2005-AVI-301

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'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-301>

Gestion du document

Référence	CERTA-2005-AVI-301
Titre	Multiples vulnérabilités d'Internet Explorer
Date de la première version	10 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-038 du 09 août 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

Execution de code arbitraire.

2 Systèmes affectés

- 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 4 ou sur Microsoft Windows XP Service Pack 1 ;
- Internet Explorer 6 sur Microsoft Windows XP Service Pack 2 ;
- Internet Explorer 6 sur Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Internet Explorer 6 sur Microsoft Windows Server 2003 (systèmes Itanium) and Microsoft Windows Server 2003 avec SP1 (systèmes Itanium) ;
- Internet Explorer 6 sur Microsoft Windows Server 2003 x64 Edition ;
- Internet Explorer 6 sur Microsoft Windows XP Professional x64 Edition ;
- Internet Explorer 5.5 Service Pack 2 sur Microsoft Windows Millennium Edition ;
- Internet Explorer 6 Service Pack 1 sur Microsoft Windows 98, sur Microsoft Windows 98 SE, ou sur Microsoft Windows Millennium Edition.

3 Résumé

De multiples vulnérabilités dans Internet Explorer permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

4 Description

Internet Explorer présente trois vulnérabilités :

- Vulnérabilité dans l'affichage des images JPEG (CAN-2005-1988) : celle-ci est due à une erreur dans la gestion de l'affichage des images JPEG permettant à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'une image malicieusement contruite.
- Vulnérabilité de type `cross-domain` (CAN-2005-1989) : celle-ci permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'une page web malicieusement construite.
- Vulnérabilité dans la gestion des objets COM (CAN-2005-1990) : celle-ci permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'une page web malicieusement construite.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS05-038 du 09 août 2005 :
<http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp>
- Référence CVE CAN-2005-1988 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1988>
- Référence CVE CAN-2005-1989 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1989>
- Référence CVE CAN-2005-1990 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1990>

Gestion détaillée du document

10 août 2005 version initiale.