



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mai 2002
N° CERTA-2002-AVI-101

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2002-AVI-101>

Gestion du document

Référence	CERTA-2002-AVI-101
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	16 mai 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-023
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

- Exécution de code arbitraire ;
- contournement des mécanismes de protection ;
- accès aux données de l'utilisateur ;
- vulnérabilité de type "Cross Site Scripting" (cf. Note d'information CERTA-2002-INF-001).

2 Systèmes affectés

- Microsoft Internet Explorer 5.01 ;
- Microsoft Internet Explorer 5.5 ;
- Microsoft Internet Explorer 6.0.

3 Résumé

Plusieurs vulnérabilités ont été mises en évidence dans le logiciel Internet Explorer de Microsoft.

4 Description

La première vulnérabilité, de type « Cross Site Scripting », permet d'exécuter du code arbitraire avec des droits privilégiés par rapport à la « Zone Internet ».

La seconde vulnérabilité permet à un concepteur de site mal intentionné, par le biais de feuilles de style judicieusement composées, de lire les données locales de la machine parcourant ce site

La troisième vulnérabilité permet, par le biais de scripts contenus dans des « cookies », d'accéder aux informations contenues dans les autres « cookies » de la machine cible.

La quatrième vulnérabilité permet à un concepteur de site d'usurper les catégories de « Zone Internet » afin de diminuer les mécanismes de protection du navigateur.

Les cinquième et sixième vulnérabilités sont des variantes de celles décrites dans l'avis CERTA-2001-AVI-163 et concernent la mauvaise gestion des en-têtes des fichiers liés aux pages HTML.

5 Solution

Télécharger le correctif sur le site Microsoft :

<http://www.microsoft.com/windows/ie/downloads/critical/Q321232/default.asp>

6 Documentation

- Bulletin Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS02-023.asp>
- Note d'information CERTA-2002-INF-001 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>
- Avis CERTA-AVI-2001-163 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-163/index.html>

Gestion détaillée du document

16 mai 2002 version initiale.