



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2002
N° CERTA-2002-AVI-248

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Correctif cumulatif pour Microsoft 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-248>

Gestion du document

Référence	CERTA-2002-AVI-248
Titre	Correctif cumulatif pour Microsoft Internet Explorer
Date de la première version	21 novembre 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-066
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

- Accès aux données ;
- contournement de la politique de sécurité ;
- déni de service.

2 Systèmes affectés

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

3 Résumé

Un correctif cumulatif concernant six vulnérabilités présentes dans Internet Explorer est disponible sur le site de Microsoft.

4 Description

- Une vulnérabilité dans la gestion des images au format PNG peut entraîner lors de la lecture d'un tel fichier l'arrêt brutal d'Internet Explorer.
- Une vulnérabilité dans l'interprétation des liens hypertextes permet, par le biais d'un lien judicieusement composé, de rediriger l'utilisateur vers un second site web en partageant les informations fournies par le client.
- Une troisième vulnérabilité permet à une personne mal intentionnée d'obtenir le nom et le chemin des fichiers temporaires utilisés par le navigateur. Cette faille ne permet pas de modifier les fichiers mais peut cependant révéler le nom de l'utilisateur ainsi que permettre l'accès aux cookies.
- Trois autres vulnérabilités permettent à un concepteur de site web mettant en ligne des pages judicieusement composées, d'obtenir l'arborescence de l'ordinateur cible. Ces vulnérabilités ne permettent pas une modification directe des données mais permettent de consulter n'importe quel dossier ou de lancer un exécutable présent sur le système local.

5 Solution

Appliquer le correctif de Microsoft disponible en téléchargement. (Cf. section Documentation)

6 Documentation

Bulletin de sécurité Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS02-066.asp>

Gestion détaillée du document

21 novembre 2002 version initiale.