



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2003
N° CERTA-2003-AVI-184

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Correctif cumulatif pour 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-2003-AVI-184>

Gestion du document

Référence	CERTA-2003-AVI-184
Titre	Correctif cumulatif pour Internet Explorer
Date de la première version	12 novembre 2003
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS03-048
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 ;
- accès aux données utilisateur.

2 Systèmes affectés

- Internet Explorer 6 Service Pack 1 ;
- Internet Explorer 6 Service Pack 1 (64-bit Edition) ;
- Internet Explorer 6 Service Pack 1 Windows Server 2003 ;
- Internet Explorer 6 Service Pack 1 Windows Server 2003 (64-bit Edition) ;
- Internet Explorer 6 Service ;
- Internet Explorer 5.5 Service Pack 2 ;
- Internet Explorer 5.01 Service Pack 4 ;
- Internet Explorer 5.01 Service Pack 3 ;
- Internet Explorer 5.01 Service Pack 2.

3 Résumé

Un correctif cumulatif pour Internet Explorer a été réalisé par Microsoft.

4 Description

- 3 vulnérabilités permettent de contourner le cloisonnement mis en place au moyen des zones de sécurité au niveau d'Internet Explorer (CVE CAN-2003-0814 ; CVE CAN-2003-815 ; CVE CAN-2003-816).
- Une vulnérabilité dans le traitement des objets XML permet à un concepteur d'un site web judicieusement composé de lire les fichiers locaux de l'utilisateur de la machine cible (CVE CAN-2003-817).
- Une vulnérabilité dans la vérification de téléchargement depuis une page DHTML permet à un concepteur de site d'effectuer un téléchargement sur la machine cible sans que l'utilisateur en soit informé par une boîte de dialogue (CVE CAN-2003-0823).

5 Solution

Appliquer le correctif de l'éditeur :

<http://www.microsoft.com/technet/security/bulletin/MS03-048.asp>

6 Documentation

- Référence CVE CAN-2003-0814 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0814>
- Référence CVE CAN-2003-0815 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0815>
- Référence CVE CAN-2003-0816 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0816>
- Référence CVE CAN-2003-0817 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0817>
- Référence CVE CAN-2003-0823 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0823>

Gestion détaillée du document

12 novembre 2003 version initiale.