



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 août 2003
N° CERTA-2003-AVI-139

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-2003-AVI-139>

Gestion du document

Référence	CERTA-2003-AVI-139
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	21 août 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS03-032 de Microsoft
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

- Microsoft Internet Explorer versions 5.01, 5.5 et 6.0 ;
- Microsoft Internet Explorer version 6.0 pour Windows Server 2003.

3 Résumé

Trois vulnérabilités présentes dans Microsoft Internet Explorer peuvent être exploitées au moyen d'un site web ou d'un message électronique au format HTML habilement constitué et permettre ainsi à un utilisateur mal intentionné d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

- Première vulnérabilité (CVE CAN-2003-0352) : Internet Explorer ne contrôle pas correctement le type de données spécifié dans l'attribut data de la balise object ;

- seconde vulnérabilité (CVE CAN-2003-0351) : lors de l'accès aux données du cache, il est possible de contourner le cloisonnement mis en place au moyen des zones de sécurité au niveau d'Internet Explorer ;
- troisième vulnérabilité (CVE CAN-2003-0350) : le contrôle ActiveX BR549.DLL présente une faille de type débordement de mémoire. Ce contrôle ActiveX est désactivé automatiquement lors de l'application du correctif.

5 Solution

Appliquer le correctif de l'éditeur :

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

6 Documentation

- Référence CVE CAN-2003-0350 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0350>
- Référence CVE CAN-2003-0351 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0351>
- Référence CVE CAN-2003-0352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352>
- Bulletin de sécurité "Internet Explorer Object Data Remote Execution Vulnerability" de eEye :
<http://www.eeye.com/html/Research/Advisories/AD20030820.html>

Gestion détaillée du document

21 août 2003 version initiale.