

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Internet Explorer 5.01 et 5.5

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-2001-AVI-055>

Gestion du document

Référence	CERTA-2001-AVI-055
Titre	Vulnérabilités dans Internet Explorer 5.01 et 5.5
Date de la première version	18 mai 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-027
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

- Usurpation de l'identité d'un serveur Web ;
- Contournement des mécanismes de sécurité.

2 Systèmes affectés

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

3 Résumé

Deux vulnérabilités ont été découvertes dans Microsoft Internet Explorer.

La première vulnérabilité concerne la vérification des certificats X.509, la seconde concerne une mauvaise interprétation des URL.

4 Description

– Première vulnérabilité :

Une fonctionnalité d'Internet Explorer permet de vérifier la validité des certificats utilisés notamment pour les sessions HTTPS/SSL (certificats X.509) par le biais de CRL (Gestion de la liste des révocations).

Une vulnérabilité présente dans cette fonctionnalité permet à un concepteur de site Web mal intentionné de contourner certaines vérifications effectuées au travers des CRL dans le but de tromper les utilisateurs sur l'identité du site.

– Deuxième vulnérabilité :

Une vulnérabilité dans l'interprétation par Internet Explorer des URL permet de faire afficher dans la barre de navigation une adresse différente de celle visualisée. Un concepteur de pages Web mal intentionné peut ainsi tromper un utilisateur distant sur l'identité de son site.

5 Solution

Télécharger le correctif sur le site Microsoft :

<http://www.microsoft.com/windows/ie/download/critical/q295106/default>

6 Documentation

Bulletin Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS01-027.asp>

Gestion détaillée du document

18 mai 2001 version initiale.