

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mauvaise vérification des certificats dans les produits Microsoft

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-202>

Gestion du document

Référence	CERTA-2002-AVI-202
Titre	Mauvaise vérification des certificats dans les produits Microsoft
Date de la première version	05 septembre 2002
Date de la dernière version	–
Source(s)	Avis #MS02-050 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

Usurpation d'identité.

2 Systèmes affectés

Tout système Windows ainsi que certains produits pour Macintosh sont vulnérables dont :

- Microsoft Windows 98 ;
- Microsoft Windows 98 Second Edition ;
- Microsoft Windows Me ;
- Microsoft Windows NT 4.0 ;
- Microsoft Windows NT 4.0, Terminal Server Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Office pour Mac ;
- Microsoft Internet Explorer pour Mac ;
- Microsoft Outlook Express pour Mac.

3 Résumé

Les produits Microsoft ne vérifient pas tous les champs des certificats utilisés pour authentifier des pages Web ou pour signer des méls. Un utilisateur mal intentionné peut générer son propre certificat permettant une usurpation d'identité.

4 Description

Les certificats au standard X.509 possèdent plusieurs champs d'options. Un de ces champs s'appelle « `Basic Constraints Field` » et indique la longueur maximum autorisée pour une chaîne de certificats ainsi que si le certificat est d'autorité ou non. Les procédures de Microsoft ne vérifient pas ce champ et donc, un certificat, habilement conçu par un utilisateur mal intentionné, peut passer pour un certificat d'autorité.

5 Solution

Appliquer le correctif de Microsoft disponible en téléchargement sur la page de l'avis #MS02-050 (Consultez la section Documentation).

6 Documentation

Avis #MS02-050 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS02-050.asp>

Gestion détaillée du document

05 septembre 2002 version initiale.