Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mars 2001
N° CERTA-2001-AVI-036

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Certificats erronés délivrés par VeriSign

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-036

Gestion du document

Référence	CERTA-2001-AVI-036
Titre	Certificats erronés délivrés par VeriSign
Date de la première version	23 mars 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft (MS01-017)
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 ;
- Coutournement des règles de sécurité.

2 Systèmes affectés

- Microsoft Windows 95 ;
- Microsoft Windows 98 ;
- Microsoft Windows Me ;
- Microsoft Windows NT 4 ;
- Microsoft Windows 2000.

3 Résumé

Suite à la délivrance par VeriSign de deux certificats au nom de Microsoft Corporation à un faux employé Microsoft, un utilisateur pourrait installer un programme ou exécuter un active X d'origine inconnue mais portant cependant la signature Microsoft.

4 Description

Les 29 et 30 janvier 2001, VeriSign a validé deux certificats à une personne se faisant passer pour un employé Microsoft. Le nom assigné à ces deux certificats est « Microsoft Corporation ».

Ces certificats peuvent être employés pour signer des programmes exécutables, des contrôles active X ou des macros. Ces programmes signés par les faux certificats peuvent être transmis par mél, téléchargés sur des pages HTML ou mis sur n'importe quel support (CD, disquette, etc...).

Ces faux certificats sont inscris dans la liste de révocation de VeriSign (CRL). Cependant, aucun point de distribution de cette liste n'étant accessible pour les certificats, il est impossible de consulter automatiquement, lors de l'installation, ces révocations.

Cet incident démontre à nouveau que la sécurité du certificat ne repose pas uniquement sur la solidité des algorithmes. La procédure appliquée par l'autorité de certification est essentielle. (Dans le cas présent VeriSign n'a pas correctement contrôlé l'identité du demandeur à priori.)

5 Contournement provisoire

Avant la mise en place d'un programme ou l'exécution d'un contrôle Active X, vérifier les dates de délivrance des certificats dans la fenêtre d'avertissement. Officiellement aucun certificat n'a été délivré pour Micorsoft en date du 29 ou 30 janvier 2001.

Un correctif Microsoft prenant en compte la vérification de ces faux certificats devrait être prochainement disponible.

6 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-017.asp

Gestion détaillée du document

23 mars 2001 version initiale.