

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Virus VBS Quatro-A

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-2000-ALE-013>

Gestion du document

Référence	CERTA-2000-ALE-013
Titre	Virus VBS Quatro-A
Date de la première version	18 septembre 2000
Date de la dernière version	–
Source(s)	Sophos Réseau de confiance
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

- Propagation de virus ;
- Perte de données.

2 Systèmes affectés

- Windows NT ;
- Windows 9x ;
- Windows 2000.

3 Résumé

VBS/Quatro-A est un virus VBS, situé dans une pièce jointe, se propageant par le carnet d'adresse d'Outlook.

4 Description

VBS/Quatro-A est du type Visual Basic Script (VBS) et arrive sous forme d'un courrier électronique proposant une mise à jour de Microsoft Internet Explorer.

Message type de présentation de ce virus :

Sujet UPDATE IEXPLORE 5.5

Corps du message La toute nouvelle version de Microsoft Internet Explorer offre de nombreux avantages aux utilisateurs et aux développeurs. Vous apprécierez en particulier la nouvelle fonction d'aperçu avant impression qui permet d'afficher les pages telles qu'elles se présenteront à l'impression. Grâce à la prise en charge améliorée des langages DHTML et CSS, les concepteurs de sites Web seront en outre plus à même de contrôler l'apparence des pages et le fonctionnement du navigateur. Téléchargez tous ces éléments aujourd'hui à partir des mises à jour de produits.

Pièce jointe UPDATE.vbs

En cas de lancement de la pièce jointe, le virus cherche des adresses e-mail dans les documents TXT, WAB, HTM et HTML de la machine cible et utilise Outlook pour se transmettre à ces adresses.

Il supprime également les fichiers de la machine cible si le fichier « c : \13A0 » n'existe pas sur cette machine.

5 Solution

- Mettre à jour votre antivirus ;
- Suivre les recommandations de la note CERTA-2000-INF-002 concernant les pièces jointes.

6 Documentation

Alerte SOPHOS :

<http://www.sophos.com/virusinfo/analyses/vbsquatroa.html>

Gestion détaillée du document

18 septembre 2000 version initiale.