Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 mars 2001
N° CERTA-2001-AVI-027

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités d'Internet Explorer et de Windows Scripting Host

Gestion du document

Référence	CERTA-2001-AVI-027
Titre	Vulnérabilités d'Internet Explorer et de Windows Scripting Host
Date de la première version	07 mars 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-015
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 ;
- Compromission des données.

2 Systèmes affectés

- Microsoft Internet Explorer s5.01 ;
- Microsoft Internet Explorer 5.5 ;
- Microsoft Windows Scripting Host 5.1 ;
- Microsoft Windows Scripting Host 5.5.

3 Résumé

Le bulletin MS01-015 de Microsoft comprend quatre vulnérabilités. Deux vulnérabilités concernent Internet Explorer, une vulnérabilité concerne Windows Scripting Host et une autre le client Telnet du service Unix 2.0.

4 Description

4.1 Première vulnérabilité

L'architecture de sécurité d'Internet Explorer fournit un mécanisme de gestion du cache afin de stocker sur la machine locale les pages internet visitées. Une vulnérabilité de ce système permet à un site distant d'avoir accès aux fichiers du cache.

Un concepteur de site mal intentionné peut, en consultant les «raccourcis» utilisés par le cache, lancer l'exécution de fichiers exécutables avec les droits de l'utilisateur local.

4.2 Deuxième vulnérabilité

Une variante des vulnérabilités décrites dans les bulletins Microsoft MS00-33, MS00-55 et MS00-093 (Référence CERTA : CERTA-2000-AVI-082) permet à un concepteur de site d'avoir accès en lecture aux fichiers se trouvant sur la machine distante.

4.3 Troisième vulnérabilité

Cette vulnérabilité identique sur le principe à la deuxième vulnérabilité concerne Microsoft Windows Scripting Host 5.1 et 5.5.

Pour connaître la version de Windows Host Scripting :

- Dans le menu Démarrer, selectionner : Rechercher fichiers ou dossiers
- Effectuer la recherche sur le fichier jscript.dll ou vbscript.dll
- Effectuer un clic droit sur le fichier trouvé afin de vérifier sa version.

4.4 Quatrième vulnérabilité

L'installation du service UNIX 2.0 permet d'intrégrer des stations Windows NT 4 et Windows 2000 dans un réseau UNIX existant. Cependant ce service, par l'intermédiaire du client Telnet fourni, apporte une vulnérabilité.

Un concepteur de site mal intentionné peut, lors de la consultation de son site, forcer Internet Explorer à utiliser le client Telnet pour télécharger un programme malicieux sur le disque de la machine distante.

5 Solution

Les différents correctifs sont téléchargeables sur le site Microsoft :

- Première et seconde vulnérabilité :
  http://www.microsoft.com/windows/ie/downloads/critical/q286045/default.asp
- troisième vulnérabilité :
  - Windows Host Scripting version 5.1 :
    http://www.microsoft.com/msdownload/vbscript/scripting51.asp
  - Windows Host Scripting version 5.5 :
    http://www.microsoft.com/msdownload/vbscript/scripting.asp
- Quatrième vulnérabilité :
  http://www.microsoft.com/windows/ie/download/critical/q286043/default.asp

6 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-015.asp

Gestion détaillée du document

07 mars 2001 version initiale.