Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 juin 2001
N° CERTA-2001-AVI-066

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des Extensions FrontPage de Microsoft IIS

Gestion du document

Référence	CERTA-2001-AVI-066
Titre	Vulnérabilité des Extensions FrontPage de Microsoft IIS
Date de la première version	26 juin 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS01-035
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 avec les privilèges d'un utilisateur normal voire de `SYSTEM`.

2 Systèmes affectés

Internet Information Server 4.0 et 5.0, installé sur les serveurs Windows NT et 2000, ayant les Extensions FrontPage activées.

3 Résumé

Une vulnérabilité d'un composant des Extensions FrontPage permet à un utilisateur mal intentionné d'exécuter du code à distance.

4 Description

Visual Studio RAD est un composant de Microsoft FrontPage Extensions qui n'est pas installé par défaut.

Un utilisateur distant mal intentionné, peu à l'aide d'une URL habilement conçue, effectuer un débordement de mémoire dans ce composant lui permettant d'exécuter du code avec les privilèges d'un utilisateur normal, ou bien ceux de `SYSTEM`.

Ces commandes sont exécutées dans le contexte de sécurité d'un utilisateur, ou bien du système, ce qui permet à l'utilsateur d'effectuer n'importe quelle action sur le serveur.

5 Contournement provisoire

Visual Studio RAD est un outils de développement des objets COM : Il ne faut pas installer Visual Studio RAD sur une machine en production.

Rendre non exécutable les librairies Dynamiques :
`Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\ISAPI\_vti_aut\fp30reg.dll`
et
`Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\bin\fp4areg.dll`.

6 Solution

Appliquer le correctif Microsoft pour les versions Anglaises et Américaines :

- Pour Windows 2000 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30727
- Pour Windows NT 4.0 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID31038

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/ms01-035.asp

Gestion détaillée du document

26 juin 2001 version initiale.