Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2003
N° CERTA-2003-AVI-187

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft FrontPage Server Extensions

Gestion du document

Référence	CERTA-2003-AVI-187
Titre	Vulnérabilités dans Microsoft FrontPage Server Extensions
Date de la première version	12 novembre 2003
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS03-051
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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

- Microsoft FrontPage Server Extensions 2000 ;
- Microsoft FrontPage Server Extensions 2002 ;
- Microsoft SharePoint Team Services 2002.

3 Résumé

Deux vulnérabilités présentes dans Microsoft FrontPage Server Extensions permettent à un utilisateur distant mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur la machine cible.

4 Description

- Microsoft FrontPage Server Extensions est un ensemble de fonctionnalités permettant notamment l'administration et la mise en ligne à distance d'un serveur Web. Une vulnérabilité dans la gestion de mémoire d'une `DLL` permet à un utilisateur distant, non authentifié, d'exécuter du code arbitraire ou de créer des comptes avec privilèges sur la machine cible (CAN-2003-0822).
- Une vulnérabilité dans l'interpréteur `SmartHTML` permet à un utilisateur distant, par le biais de requêtes judicieusement composées, de réaliser un déni de service en bloquant le traitement par le serveur de toutes les requêtes suivantes (CAN-2003-0824).

5 Solution

Appliquer le correctif de l'éditeur :
http://www.microsoft.com/technet/security/bulletin/MS03-051.asp

6 Documentation

- Référence CVE CAN-2003-0822 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0822
- Référence CVE CAN-2003-0824 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0824

Gestion détaillée du document

12 novembre 2003 version initiale.