Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2002
N° CERTA-2002-AVI-044

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Commerce Server 2000

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-2002-AVI-044

Gestion du document

Référence	CERTA-2002-AVI-044
Titre	Vulnérabilité dans Microsoft Commerce Server 2000
Date de la première version	22 février 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS02-010
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 à distance.

2 Systèmes affectés

Microsoft Commerce Server 2000.

3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire en exploitant une vulnérabilité du filtre `AuthFilter`.

4 Description

Les filtres ISAPI sont des programmes qui répondent à des requêtes HTTP reçues par le serveur WEB. Microsoft Commerce Server installe une bibliothèque dynamique (DLL) Windows avec le filtre ISAPI `AuthFilter` qui permet l'utilisation de différentes méthodes d'authentification.

Le filtre `AuthFilter` contient un débordement de mémoire dans la partie traitant la manipulation de ces authentifications. Un utilisateur mal intentionné peut effectuer un débordement de mémoire afin de stopper le service commerce server ou d'exécuter du code arbitraire avec les privilèges `LocalSystem`.

5 Solution

Appliquer le correctif de sécurité fournit par Microsoft :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=36683

6 Documentation

Bulletin de sécurité de Microsoft MS02-010 :
http://www.microsoft.com/technet/security/bulletin/MS02-010.asp

Gestion détaillée du document

22 février 2002 version initiale.