



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2004
N° CERTA-2004-AVI-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Internet Security and Acceleration 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-2004-AVI-004>

Gestion du document

Référence	CERTA-2004-AVI-004
Titre	Vulnérabilité de Microsoft Internet Security and Acceleration Server 2000
Date de la première version	14 janvier 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-01 de Microsoft Avis de sécurité 006489/H323 du NISCC
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 Internet Security and Acceleration Server 2000.

Les produits suivants contenant Microsoft Internet Security and Acceleration Server 2000 sont également concernés :

- Microsoft Small Business Server 2000 ;
- Microsoft Small Business Server 2003.

3 Résumé

Une vulnérabilité présente dans Microsoft Internet Security and Acceleration Server 2000 peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

H.323 est un protocole utilisé par les applications de téléphonie sur IP.

Une vulnérabilité de type débordement de mémoire présente dans le filtre H.323 peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire dans le contexte du service Microsoft Firewall.

Seules les plate-formes ISA Server fonctionnant en mode pare-feux (Firewall) sont vulnérables. Le filtre H.323 est activé par défaut dans ce mode.

5 Contournement provisoire

Dans l'attente de l'application du correctif, désactiver le filtre H.323 sur la plate-forme Microsoft ISA Server 2000.

6 Solution

Se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

7 Documentation

- Bulletin de sécurité MS04-001 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS04-001.asp>
- Avis de sécurité 006489/H323 du NISCC :
<http://www.uniras.gov.uk/vuls/2004/006489/h323.htm>

Gestion détaillée du document

14 janvier 2004 version initiale.