



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 juin 2005  
N° CERTA-2005-AVI-215

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Microsoft ISA 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-2005-AVI-215>

---

### Gestion du document

Référence	CERTA-2005-AVI-215
Titre	Vulnérabilité de Microsoft ISA Server 2000
Date de la première version	15 juin 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-034 du 14 juin 2005
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

Elévation de privilèges.

## 2 Systèmes affectés

- Microsoft Internet Security and Acceleration (ISA) Server 2000 Standard Edition ;
- Microsoft Internet Security and Acceleration (ISA) Server 2000 Enterprise Edition.

## 3 Résumé

Une vulnérabilité dans Microsoft ISA Server 2000 permet à un utilisateur mal intentionné d'élever ses privilèges.

## 4 Description

- Une première vulnérabilité dans le traitement des requêtes HTTP mal formées permet à un utilisateur mal intentionné de corrompre le cache du serveur ISA affecté (CVE CAN-2005-1215) ;

- une seconde vulnérabilité dans le filtre prédéfini NETBIOS permet à un utilisateur mal intentionné d'élever ses privilèges (CVE CAN-2005-1216).

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Microsoft MS05-034 du 14 juin 2005 :  
<http://www.microsoft.com/france/technet/securite/ms05-034.msp>
- Référence CVE CAN-2005-1215 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1215>
- Référence CVE CAN-2005-1216 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1216>

## **Gestion détaillée du document**

**15 juin 2005** version initiale.