

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans ISA Server

---

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-2003-AVI-113>

---

### Gestion du document

Référence	CERTA-2003-AVI-113
Titre	Vulnérabilité dans ISA Server
Date de la première version	17 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS03-028 de Microsoft
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.

## 2 Systèmes affectés

– Microsoft Internet Security and Acceleration (ISA) Server 2000.

## 3 Résumé

Des vulnérabilités de type `cross-site scripting` sont présentes dans plusieurs pages retournées par le serveur ISA lors de certaines erreurs spécifiques.

## 4 Description

Microsoft ISA (Internet Security and Acceleration) Server 2000 est un garde-barrière ainsi qu'un serveur mandataire. Il permet notamment de filtrer le trafic au niveau applicatif.

La fonction `homepage ( )` dans plusieurs pages d'erreur de ISA Server ne code pas correctement les URL en texte HTML.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire sur un poste client accédant au server ISA vulnérable au travers de son navigateur (vulnérabilité de type cross-site scripting).

## **5 Solution**

Appliquer le correctif fourni par Microsoft (cf. Documentation).

## **6 Documentation**

Bulletin de sécurité #MS03-028 de Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms03-028.asp>

Note d'information CERTA-2002-INF-01 du CERTA :

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>

Référence CVE CAN-2003-0526 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0526>

## **Gestion détaillée du document**

**17 juillet 2003** version initiale.