



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 novembre 2004
N° CERTA-2004-AVI-365

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ISA Server / Proxy 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-2004-AVI-365>

Gestion du document

Référence	CERTA-2004-AVI-365
Titre	Vulnérabilité dans ISA Server / Proxy Server
Date de la première version	10 novembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-039
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Usurpation d'adresse réticulaire (URL).

2 Systèmes affectés

- Microsoft Proxy Server 2.0 Service Pack 1 ;
- Microsoft Internet Security and Acceleration Server 2000 Service Pack 1 & 2 ;
- Microsoft Small Business Server 2000 ;
- Microsoft Small Business Server 2003 Premium Edition.

3 Résumé

Une vulnérabilité découverte dans les systèmes affectés de Microsoft permet à un utilisateur mal intentionné d'usurper l'adresse réticulaire (URL) d'un site web.

4 Description

Les produits ISA Server 2000 et Proxy Server 2.0 enregistrent dans un cache les réponses des requêtes DNS inverse, et utilisent ce cache pour résoudre les requêtes DNS. Une personne mal intentionnée peut, par le biais d'une requête DNS inverse malicieusement construite, polluer le cache en vue de duper un internaute en lui faisant croire qu'il accède à un site web de confiance tandis qu'il sera dirigé vers un site web malicieux.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS04-039 du 09 novembre 2004 :
<http://www.microsoft.com/technet/security/bulletin/MS04-039.mspx>
- Référence CVE CAN-2004-0892 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0892>

Gestion détaillée du document

10 novembre 2004 version initiale.