

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Winsock Proxy Service et de Microsoft ISA Firewall Service

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-075>

Gestion du document

Référence	CERTA-2003-AVI-075
Titre	Vulnérabilité de Microsoft Winsock Proxy Service et de Microsoft ISA Firewall Service
Date de la première version	11 avril 2003
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS03-012
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

Déni de service.

2 Systèmes affectés

- Microsoft Proxy Server 2.0
- Microsoft Internet Security and Acceleration (ISA) Server 2000.

Les systèmes utilisant Microsoft ISA Server 2000 uniquement en mode cache ne sont pas affectés puisque le service Microsoft ISA Firewall n'est pas activé par défaut.

3 Résumé

Une vulnérabilité dans Winsock Proxy Service de Microsoft Proxy Server 2.0 et dans Microsoft Firewall Service de Microsoft ISA Server 2000 permet à un utilisateur mal intentionné du réseau local de créer un déni de service.

4 Description

Microsoft Proxy Server est un serveur mandataire et Microsoft ISA Server est un garde-barrière. Tous deux gèrent les protocoles applicatifs tels FTP, Telnet, SMTP etc. Une vulnérabilité dans Winsock Proxy Service et dans Microsoft Firewall Service permet à un utilisateur mal intentionné du réseau local de créer un déni de service en envoyant un paquet judicieusement construit. Les deux serveurs seront alors dans l'incapacité de répondre aux requêtes provenant du réseau interne et du réseau externe.

5 Solution

Appliquer les correctifs fournis par Microsoft :

- Microsoft Proxy Server 2.0 :
<http://microsoft.com/downloads/details.aspx?FamilyId=C81688B7-20FB-45EB-BAFD-031A0D2923E6&displaylang=fr>
- Microsoft ISA Server 2000 :
<http://microsoft.com/downloads/details.aspx?FamilyId=3C43FAD2-A888-4603-84B7-1053C8663436&displaylang=fr>

6 Documentation

- Bulletin de sécurité Microsoft MS03-012 :
<http://www.microsoft.com/technet/security/bulletin/MS03-12.asp>
- Référence CVE CAN-2003-0110 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0110>

Gestion détaillée du document

11 avril 2003 version initiale.