

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft 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-2009-AVI-146>

Gestion du document

Référence	CERTA-2009-AVI-146
Titre	Vulnérabilité dans Microsoft ISA Server
Date de la première version	15 avril 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-016 du 14 avril 2009
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 à distance ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Microsoft Forefront Management Gateway, Medium Business Edition ;
- Microsoft Internet Security and Acceleration Server 2004 Standard Edition Service Pack 3 ;
- Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition Service Pack 3 ;
- Microsoft Internet Security and Acceleration Server 2006 ;
- Microsoft Internet Security and Acceleration Server 2006 Support Update ;
- Microsoft Internet Security and Acceleration Server 2006 Service Pack 1.

3 Résumé

Plusieurs vulnérabilités présentes dans Microsoft ISA Server et Microsoft Forefront Management Gateway permettent à un utilisateur distant de provoquer un déni de service ou de réaliser des attaques de type injection de code indirecte (*Cross-site Scripting*).

4 Description

Deux vulnérabilités sont présentes dans Microsoft ISA Server et Microsoft Forefront Management Gateway :

- la première est relative à une erreur dans la gestion des états TCP par le pare-feu pour les services Web proxy et Web publishing. Elle permet à un utilisateur distant de provoquer un déni de service (CVE-2009-0077) ;
- la seconde concerne une erreur dans les formulaires HTML d'authentification de ISA Server et Forefront TMG. Elle permet à un utilisateur distant de réaliser des attaques de type injection de code indirecte (*Cross-site Scripting*) (CVE-2009-0237).

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 M09-016 du 14 avril 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/M09-016.mspx>
<http://www.microsoft.com/technet/security/Bulletin/M09-016.mspx>
- Référence CVE CVE-2009-0077 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0077>
- Référence CVE CVE-2009-0237 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0237>

Gestion détaillée du document

15 avril 2009 version initiale.