

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le composant SMTP de Windows Server 2003

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-339>

Gestion du document

Référence	CERTA-2004-AVI-339
Titre	Vulnérabilité dans le composant SMTP de Windows Server 2003
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-035 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 à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Les applications suivantes sont affectées :

- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition ;
- Microsoft Exchange Server 2003 et Microsoft Exchange Server 2003 Service Pack 1 installé sur une plate-forme Windows Server 2003 ;
- Microsoft Exchange Server 2003 installé sur une plate-forme Windows 200 SP 3 ou SP4.

3 Description

Une vulnérabilité est présente dans la mise en œuvre du traitement des requêtes DNS (Domain Name System) par les composants Windows Server 2003 SMTP et Microsoft Exchange Server 2003 Routing Engine. Cette vulnérabilité peut être exploitée par un individu mal intentionné afin de prendre le contrôle du serveur affecté par l'envoi de requêtes DNS malicieusement construites.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS04-035 du 12 octobre 2004 :
<http://www.microsoft.com/technet/security/bulletin/MS04-035.msp>
- Référence CVE CAN-2004-0840 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0840>

Gestion détaillée du document

13 octobre 2004 version initiale.