



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mai 2007
N° CERTA-2007-AVI-206

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Exchange

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-2007-AVI-206>

Gestion du document

Référence	CERTA-2007-AVI-206
Titre	Multiples vulnérabilités dans Microsoft Exchange
Date de la première version	09 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-026 du 8 mai 2007
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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Exchange Server 2000 Service Pack 3 (avec le Post-Service Pack 3 rollup du mois d'août 2004) ;
- Microsoft Exchange Server 2003 Service Pack 1 ;
- Microsoft Exchange Server 2003 Service Pack 2 ;
- Microsoft Exchange Server 2007.

3 Résumé

Plusieurs vulnérabilités présentes dans Microsoft Exchange Server permettent d'exécuter du code arbitraire à distance ou de réaliser un déni de service.

4 Description

Quatre vulnérabilités sont présentes dans Microsoft Exchange Server :

- la première concerne Outlook Web Access (AWO), une personne malintentionnée peut exécuter du code arbitraire par le biais d'un courriel spécialement conçu ;
- la seconde affecte Exchange Collaboration Data Objects (EXCDO), un déni de service à distance peut être réalisé par le biais d'un courriel contenant un fichier iCal, concernant le calendrier et la planification, spécialement formaté ;
- la troisième concerne la gestion des formats MIME, une personne malveillante peut exécuter du code arbitraire par le biais d'un courriel spécialement conçu encodé en Base64 ;
- la dernière vulnérabilité concerne la gestion des requêtes IMAP, un déni de service peut être réalisé par le biais d'une requête IMAP spécialement conçue.

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 MS07-026 du 08 mai 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-026.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS07-026.mspx>
- Référence CVE CVE-2007-0220 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0220>
- Référence CVE CVE-2007-0039 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0039>
- Référence CVE CVE-2007-0213 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0213>
- Référence CVE CVE-2007-0221 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0221>

Gestion détaillée du document

09 mai 2007 version initiale.