

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel Ipswitch IMail 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-2006-AVI-395>

Gestion du document

Référence	CERTA-2006-AVI-395
Titre	Vulnérabilité du logiciel Ipswitch IMail server
Date de la première version	14 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de mise à jour Ipswitch du 06 septembre 2006
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.

2 Systèmes affectés

- Imail Secure Server 2006 ;
- Imail Server 2006 ;
- Ipswitch Collaboration Suite 2006.

3 Résumé

Une vulnérabilité permettant l'exécution de code arbitraire à distance a été découverte dans IMail server.

4 Description

Une vulnérabilité due à une erreur lors du traitement de certaines chaînes de caractères par le service SMTP a été découverte dans IMail server, ainsi que dans les logiciels Ipswitch utilisant cette brique applicative.

Cette vulnérabilité peut être exploitée à distance par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la machine vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (version 2006.1, cf. section Documentation).

6 Documentation

- Site de l'éditeur :
<http://www.ipswitch.com>
- Bulletin de mise à jour de l'éditeur :
<http://www.ipswitch.com/support/ics/updates/ics20061.asp>
<http://www.ipswitch.com/support/imap/releases/im20061.asp>
- Référence CVE CVE-2006-4379 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4379>

Gestion détaillée du document

14 septembre 2006 version initiale.