

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Ipswitch Imail

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-2005-AVI-185>

Gestion du document

Référence	CERTA-2005-AVI-185
Titre	Multiples vulnérabilités de Ipswitch Imail
Date de la première version	30 mai 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité iDEFENSE du 24 mai 2005
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 ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Ipswitch Imail versions 8.13 et antérieures.

3 Résumé

Plusieurs vulnérabilités découvertes dans Ipswitch Imail permettent d'exécuter du code arbitraire à distance, de réaliser un déni de service, ou de lire n'importe quel fichier sur le serveur.

4 Description

Le serveur Ipswitch Imail est un serveur de messagerie inclus dans Ipswitch Collaboration Suite (ICS).

Plusieurs vulnérabilités ont été découvertes dans Ipswitch Imail :

- une vulnérabilité affecte le traitement des paramètres passés à la commande SELECT du serveur IMAP d'Ipswitch Imail. En envoyant des paramètres de 260 octets environ, il est possible de provoquer un arrêt brutal du serveur IMAP (référence CVE CAN-2005-1254) ;
- une vulnérabilité de type « traversée de répertoires » dans le serveur Web Calendaring d'Ipswitch Imail permet d'accéder en lecture à tous les fichiers du système (référence CVE CAN-2005-1252) ;
- deux vulnérabilités affectent la commande LOGIN du serveur IMAP d'Ipswitch Imail. En fournissant un nom d'utilisateur de 2000 octets environ ou débutant avec un caractère spécial, un utilisateur mal intentionné peut exécuter du code arbitraire à distance (référence CVE CAN-2005-1255) ;
- une vulnérabilité affecte la commande STATUS du serveur IMAP d'Ipswitch Imail. En fournissant un long nom de boîte aux lettres en paramètre de la commande STATUS, un utilisateur mal intentionné préalablement authentifié peut exécuter du code arbitraire à distance (référence CVE CAN-2005-1256) ;
- une vulnérabilité est présente dans le traitement des commandes LSUB. Un utilisateur mal intentionné peut réaliser un déni de service sur le serveur IMAP d'Ipswitch Imail en envoyant une longue chaîne de caractères NULL à la directive LSUB (référence CVE CAN-2005-1249).

5 Solution

Appliquer le correctif de l'éditeur (cf. section Documentation).

6 Documentation

- Bulletin de sécurité d'Ipswitch du 23 mai 2005 :
http://www.ipswitch.com/support/imap/releases/imap_professional/im82hf2.html
- Bulletin de sécurité iDEFENSE du 24 mai 2005 « Ipswitch IMail IMAP SELECT Command DoS Vulnerability » :
<http://www.odefense.com/application/poi/display?id=241&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE du 24 mai 2005 « Ipswitch IMail Web Calendaring Arbitrary File Read Vulnerability » :
<http://www.odefense.com/application/poi/display?id=242&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE du 24 mai 2005 « Ipswitch IMail IMAP LOGIN Remote Buffer Overflow Vulnerabilities » :
<http://www.odefense.com/application/poi/display?id=243&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE du 24 mai 2005 « Ipswitch IMail STATUS Remote Buffer Overflow Vulnerability » :
<http://www.odefense.com/application/poi/display?id=244&type=vulnerabilities>
- Bulletin de sécurité iDEFENSE du 24 mai 2005 « Ipswitch IMail IMAP LSUB DoS Vulnerability » :
<http://www.odefense.com/application/poi/display?id=245&type=vulnerabilities>
- Référence CVE CAN-2005-1249 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1249>
- Référence CVE CAN-2005-1252 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1252>
- Référence CVE CAN-2005-1254 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1254>
- Référence CVE CAN-2005-1255 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1255>
- Référence CVE CAN-2005-1256 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1256>

Gestion détaillée du document

30 mai 2005 version initiale.