Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 septembre 2003
N° CERTA-2003-AVI-150-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du client de messagerie Pine

Gestion du document

Référence	CERTA-2003-AVI-150-001
Titre	Vulnérabilités du client de messagerie Pine
Date de la première version	11 septembre 2003
Date de la dernière version	12 septembre 2003
Source(s)	Avis de sécurité iDEFENSE 09.10.03
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

Pine versions 4.56 et antérieures.

3 Résumé

Deux vulnérabilités dans le client de messagerie Pine permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Pine est un client de messagerie textuel développé par l'Université de Washington. Deux vulnérabilités de type débordement de mémoire sont présentes dans le traitement des messages électroniques par Pine. La première vulnérabilité est une mauvaise gestion du champ `message/external-body` de l'en-tête des messages. La seconde vulnérabilité est un débordement de mémoire dans la fonction `rfc2231_get_param()`. Il est ainsi

possible pour un utilisateur mal intentionné d'exécuter du code arbitraire à distance par l'envoi d'un message électronique judicieusement composé.

5 Solution

Mettre à jour Pine en version 4.58. La nouvelle version de Pine peut être obtenue à l'adresse suivante : http://www.washigton.edu/pine/getpine/

6 Documentation

- Avis de sécurité iDEFENSE 09.10.03 : http://www.idefense.com/advisory/09.10.03.txt
- Site Pine à l'Université de Washington : http://www.washington.edu/pine/
- Avis de sécurité RedHat RHSA-2003:273-01 : https://rhn.redhat.com/errata/RHSA-2003-273.html
- Avis de sécurité SuSE SuSE-SA:2003:037 : http://www.suse.de/de/security/2003_037_pine.html
- Avis de sécurité Slackware SSA:2003-253-01 : http://www.slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.347016
- Référence CVE CAN-2003-0720 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0720
- Référence CVE CAN-2003-0721 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0721

Gestion détaillée du document

11 septembre 2003 version initiale.
12 septembre 2003 ajout références aux bulletins de sécurité de RedHat, SuSE et Slackware.