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 septembre 2004
N° CERTA-2004-AVI-269-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de gaim

Gestion du document

Référence	CERTA-2004-AVI-269-001
Titre	Vulnérabilité de gaim
Date de la première version	16 août 2004
Date de la dernière version	09 septembre 2004
Source(s)	Bulletin de sécurité SuSE SUSE-SA:2004:025 du 12 août 2004
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.

2 Systèmes affectés

gaim versions 0.81 et antérieures.

3 Résumé

Une vulnérabilité de *gaim* permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

4 Description

gaim est un client de messagerie instantanée multi-protocoles (ICQ, MSN Messenger, Yahoo!, IRC, Jabber, AIM, ...).

Une vulnérabilité de type débordement de mémoire a été découverte dans l'application *gaim*.

Elle permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire avec les privilèges de l'utilisateur ayant lancé *gaim*, par le simple envoi d'un message malicieusement construit.

5 Solution

La version 0.81-r1 corrige cette vulnérabilité.

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

6 Documentation

- Site Internet de *gaim* :
  http://gaim.sourceforge.net
- Bulletin de sécurité Gentoo GLSA-200408-12 du 12 août 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200408-12.xml
- Bulletin de sécurité Mandrake MDKSA-2004:081 du 12 août 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:081
- Bulletin de sécurité SuSE SUSE-SA:2004:025 du 12 août 2004 :
  http://www.suse.com/de/security/2004_25_gaim.html
- Bulletin de sécurité FreeBSD pour gaim du 12 août 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité RedHat RHSA-2004:400 du 07 septembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-400.html
- Référence CVE CAN-2004-0500 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0500
- Recommandation CERTA-2002-REC-001 du 28 mars 2002 sur l'usage de la messagerie instantanée ou de l'IRC :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-001/index.html

Gestion détaillée du document

16 août 2004 version initiale.
09 septembre 2004 ajout de la référence au bulletin de sécurité RedHat.