Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2004
N° CERTA-2004-AVI-350-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Gaim

Gestion du document

Référence	CERTA-2004-AVI-350-003
Titre	Multiples vulnérabilités de Gaim
Date de la première version	21 octobre 2004
Date de la dernière version	22 novembre 2004
Source(s)	Bulletin de sécurité RHSA-2004:604 de Red Hat
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.

2 Systèmes affectés

gaim versions 1.0.1 et antérieures.

3 Résumé

De multiples vulnérabilités présentes dans `gaim` permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance ou réaliser un déni de service sur le poste client vulnérable.

4 Description

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

MSNSLP est un protocole utilisé par le logiciel de messagerie instantanée MSN Messenger.

Une vulnérabilité de type débordement de mémoire est présente dans une des routines traitant les messages au format MSNSLP. Par le biais de messages habilement constitués, un utilisateur distant mal intentionné peut exécuter du code arbitraire à distance sur un client `gaim` vulnérable.

Deux autres vulnérabilités pouvant entrainer un déni de service par arrêt brutal de l'application sont également présente dans `gaim`.

5 Solution

La version 1.0.2 de `gaim` corrige ces vulnérabilités.

6 Documentation

- Sources de gaim :
  http://gaim.sourceforge.net
- Bulletin "MSN SLP buffer overflow" du 19 octobre 2004 :
  http://gaim.sourceforge.net/security/?id=9
- Bulletin "MSN SLP DOS" du 19 octobre 2004 :
  http://gaim.sourceforge.net/security/?id=8
- Bulletin "MSN file transfer DOS" du 19 octobre 2004 :
  http://gaim.sourceforge.net/security/?id=7
- Bulletin de sécurité RHSA-2004:604 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2004-604.html
- Bulletin de sécurité Gentoo GLSA-200410-23 du 24 octobre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200410-23.xml
- Bulletin de sécurité Mandrake MDKSA-2004:117 du 01 novembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:117
- Bulletin de sécurité OpenBSD pour gaim du 22 octobre 2004 :
  http://www.vuxml.org/openbsd/
- Référence CVE CAN-2004-0891 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0891

Gestion détaillée du document

21 octobre 2004 version initiale.

27 octobre 2004 ajout de la référence au bulletin de sécurité Gentoo.

04 novembre 2004 ajout de la référence au bulletin de sécurité Mandrake.

22 novembre 2004 ajout référence au bulletin de sécurité OpenBSD.