Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 juin 2005
N° CERTA-2005-AVI-163-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de gaim

Gestion du document

Référence	CERTA-2005-AVI-163-002
Titre	Multiples vulnérabilités de gaim
Date de la première version	13 mai 2005
Date de la dernière version	14 juin 2005
Source(s)	Bulletins de sécurité #16 et #17 de gaim
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 antérieures à la 1.3.0.

3 Résumé

Deux 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, ...).

Une vulnérabilité de type débordement de mémoire est présente lors du traitement d'URLS malicieusement constituées (CVE CAN-2005-161). En exploitant cette vulnérabilité, un utilisateur distant mal intentionné peut exécuter du code arbitraire à distance sur un client `gaim` vulnérable.

Une autre vulnérabilité (CVE CAN-2005-162) pouvant entrainer un déni de service par arrêt brutal de l'application est également présente dans `gaim` lors du traitement de certains messages MSNSLP (utilisé par le logiciel de messagerie instantanée MSN Messenger).

5 Solution

La version 1.3.0 de `gaim` corrige ces vulnérabilités.

6 Documentation

- Sources de gaim :
  http://gaim.sourceforge.net
- Bulletin "Remote crash on some protocols" du 10 mai 2005 :
  http://gaim.sourceforge.net/security/?id=16
- Bulletin "MSN remote Dos" du 10 mai 2005 :
  http://gaim.sourceforge.net/security/?id=17
- Bulletin de sécurité RedHat RHSA-2005:429 du 10 mai 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-429.html
- Bulletin de sécurité RedHat RHSA-2005:432 du 11 mai 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-432.html
- Bulletin de sécurité Gentoo GLSA 200505-09 du 12 mai 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200505-09.xml
- Bulletin de sécurité Mandriva MDKSA-2005:086 du 12 mai 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:086
- Mise à jour de sécurité pour Fedora Core 3 du 12 mai 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
- Bulletin de sécurité pour OpenBSD "gaim – multiples vulnerabilities" du 13 mai 2005 :
  http://www.vuxml.org/openbsd/
- Bulletin de sécurité pour FreeBSD "gaim – MSN remote DoS vulnerability" du 14 mai 2005 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité pour FreeBSD "gaim – remote crash on some protocols" du 14 mai 2005 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité SUSE SUSE-SR:2005:015 du 07 juin 2005 :
  http://www.novell.com/linux/security/advisories/2005_15_sr.html
- Référence CVE CAN-2005-1261 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1261
- Référence CVE CAN-2005-1262 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1262

Gestion détaillée du document

13 mai 2005 version initiale.

03 juin 2005 ajout des bulletins de sécurité pour OpenBSD et FreeBSD.

14 juin 2005 ajout des références aux bulletins de sécurité SUSE et RedHat RHSA-2005:432.