Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 août 2005
N° CERTA-2005-AVI-311-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Gaim

Gestion du document

Référence	CERTA-2005-AVI-311-002
Titre	Multiples vulnérabilités dans Gaim
Date de la première version	12 août 2005
Date de la dernière version	31 août 2005
Source(s)	Bulletin de sécurité 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 version 1.4.0 et version antérieures.

3 Description

Les trois vulnérabilités suivantes ont été découverte dans le logiciel Gaim :

- Un débordement de pile dans la gestion des messages d'abscence d'AIM et ICQ peut être utilisé par une personne mal intentionnée pour exécuter du code arbitraire à distance ;
- une mauvaise gestion dans le processus d'envoi de fichier permet à un utilisateur mal intentionnée de stopper à distance le logiciel grâce à l'envoi d'un fichier dont le nom aurait été malicieusement construit ;
- une mauvaise gestion des messages permet à un utilisateur mal intentionnée de stopper à distance le logiciel grâce à l'envoi d'un message malicieusement construit. Cette vulnérabilité n'affecte que les versions de Gaim conçues pour les systèmes PPC et IBM S/390.

4 Solution

Mettre à jour en version 1.5.0 :
http://gaim.sourceforge.net/downloads.php

5 Documentation

- Site de l'éditeur :
  http://gaim.sourceforge.net
- Bulletin de sécurité Gaim :
  http://gaim.sourceforge.net/security/index.php?id=21
- Bulletin de sécurité Red Hat :
  http://rhn.redhat.com/errata/RHSA-2005-627.html
- Bulletin de sécurité Mandriva MDKSA-2005:139 du 15 août 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:139
- Bulletin de sécurité Gentoo GLSA-200508-06 du 15 août 2005 :
  http://security.gentoo.org/glsa/glsa-200508-06.xml
- Bulletin de sécurité SuSE du 19 août 2005 :
  http://www.novell.com/linux/security/advisories/2005_19_sr.html
- Référence CAN-CVE : CAN-2005-2102
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2102
- Référence CAN-CVE : CAN-2005-2103
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2103
- Référence CAN-CVE : CAN-2005-2370
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2370
- Bulletin de sécurité OpenBSD :
  http://www.vuxml.org/openbsd/pkg-gaim.html
- Bulletin de sécurité FreeBSD :
  http://www.vuxml.org/freebsd/pkg-gaim.html

Gestion détaillée du document

12 août 2005 version initiale.
18 août 2005 ajout des bulletins de sécurité OpenBSD et FreeBSD.
31 août 2005 ajout des bulletins de sécurité Mandriva, Gentoo et SuSE.