



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2005
N° CERTA-2005-AVI-202-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Gaim

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-202>

Gestion du document

Référence	CERTA-2005-AVI-202-005
Titre	Multiples vulnérabilités de Gaim
Date de la première version	13 juin 2005
Date de la dernière version	13 juillet 2005
Source(s)	Bulletin de sécurité Gaim du 10 juin 2005
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

Déni de service.

2 Systèmes affectés

gaim versions antérieures à la 1.3.1.

3 Résumé

Deux vulnérabilités présentes dans gaim permettent à un utilisateur distant mal intentionné de 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, ...).

Deux vulnérabilités présentes dans le traitement des noms de fichiers via Yahoo! (CVE CAN-2005-269) ou le traitement de certains messages via MSN (CVE CAN-2005-1934) peuvent être exploitées par un utilisateur distant mal intentionné afin de réaliser un déni de service sur le poste client vulnérable.

5 Solution

La version 1.3.1 de `gaim` corrige ces vulnérabilités.

6 Documentation

- Sources de `gaim` :
<http://gaim.sourceforge.net>
- Bulletin "Remote Yahoo! crash" du 10 juin 2005 :
<http://gaim.sourceforge.net/security/?id=18>
- Bulletin "MSN remote Dos" du 10 juin 2005 :
<http://gaim.sourceforge.net/security/?id=19>
- Bulletin de sécurité Gentoo GLSA 200506-11 du 12 juin 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200506-11.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:099 du 14 juin 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:099>
- Bulletin de sécurité RedHat RHSA-2005:518 du 16 juin 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-518.html>
- Bulletins de sécurité FreeBSD pour `gaim`, `ja-gaim`, `ko-gaim` et `ru-gaim` du 17 juin 2005 :
<http://www.vuxml.org/freebsd/pkg-gaim.html>
- Bulletin de sécurité Debian DSA-734 du 05 juillet 2005 :
<http://www.debian.org/security/2005/dsa-734>
- Bulletin de sécurité SUSE SUSE-SR:2005:017 du 13 juillet 2005 :
http://www.novell.com/linux/security/advisories/2005_17_sr.html
- Référence CVE CAN-2005-1269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1269>
- Référence CVE CAN-2005-1934 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1934>

Gestion détaillée du document

13 juin 2005 version initiale.

15 juin 2005 ajout de la référence au bulletin de sécurité Mandriva.

17 juin 2005 ajout de la référence au bulletin de sécurité RedHat.

20 juin 2005 ajout des références aux bulletins de sécurité FreeBSD.

06 juillet 2005 ajout de la référence au bulletin de sécurité Debian.

13 juillet 2005 ajout de la référence au bulletin de sécurité SUSE.