



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 avril 2005  
N° CERTA-2005-AVI-142

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-142>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2005-AVI-142  |
| Titre                       | Multiples vulnérabilités dans GAIM  |
| Date de la première version | 15 avril 2005   |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de sécurité de l'éditeur Gaim du 04 avril 2005<br>Bulletins de sécurité de l'éditeur Gaim du 02 avril 2005 |
| Pièce(s) jointe(s)          |   |

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

Versions antérieures à Gaim 1.2.1.

## 3 Résumé

De multiples vulnérabilités découvertes dans Gaim permettent à un utilisateur mal intentionné d'effectuer un déni de service à distance.

## 4 Description

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

- une vulnérabilité découverte dans la fonction `gaim_markup_strip_html()` permet à un individu mal intentionné de provoquer un déni de service au moyen d'une chaîne contenant du code HTML astucieusement formé (CAN-2005-0965).
- une vulnérabilité dans le module de gestion du protocole IRC permet à un utilisateur mal intentionné de forcer à distance la fermeture de l'application (CAN-2005-0966) ;
- Une vulnérabilité découverte dans `gaim` permet à un utilisateur Jabber mal intentionné d'effectuer un déni de service sur le client `gaim`, au moyen d'une requête de transfert de fichier malicieusement construite (CAN-2005-0967) ;

## 5 Solution

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

## 6 Documentation

- Sources de `gaim` :  
<http://gaim.sourceforge.net>
- Mise à jour Gaim 1.2.1 :  
<http://gaim.sourceforge.net/downloads.php>
- Bulletin de sécurité `gaim` #13 du 02 avril 2005 :  
<http://gaim.sourceforge.net/security/index.php?id=13>
- Bulletin de sécurité `gaim` #14 du 02 avril 2005 :  
<http://gaim.sourceforge.net/security/index.php?id=14>
- Bulletin de sécurité `gaim` #15 du 04 avril 2005 :  
<http://gaim.sourceforge.net/security/index.php?id=15>
- Bulletin de sécurité Gentoo GLSA-200504-05 / Gaim du 06 avril 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200504-05.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:071 du 13 avril 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:071>
- Bulletin de sécurité RedHat RHSA-2005:365:06 du 12 avril 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-365.html>
- Mise à jour de sécurité pour Fedora Core 2 / Gaim du 06 avril 2005 :  
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité pour Fedora Core 3 / Gaim du 06 avril 2005 :  
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité FreeBSD pour Gaim du 10 avril 2004 :  
<http://www.vuxml.org/freebsd/pkg-gaim.html>
- Référence CVE CAN-2005-0965 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0965>
- Référence CVE CAN-2005-0966 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0966>
- Référence CVE CAN-2005-0967 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0967>

## Gestion détaillée du document

15 avril 2005 version initiale.