



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 mars 2005  
N° CERTA-2005-AVI-102-001

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-102>

---

### Gestion du document

Référence	CERTA-2005-AVI-102-001
Titre	Multiples vulnérabilités dans GAIM
Date de la première version	08 mars 2005
Date de la dernière version	11 mars 2005
Source(s)	Bulletins de sécurité de l'éditeur Gaim
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

Gaim 1.1.3 et versions antérieures.

## 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 erreur dans l'analyse syntaxique des paquets SNAC permet à un individu mal intentionné d'effectuer un déni de service sur l'application au moyen de paquets malicieusement construits (CAN-2005-0472) ;

- une vulnérabilité dans le traitement de code HTML (HyperText Markup Language) peut être exploitée au moyen d'un code HTML malicieusement constitué afin d'exécuter un déni de service (CAN-2005-0473) ;
- une vulnérabilité découverte dans la fonction "enregistrer sous ..." permet à un utilisateur distant mal intentionné d'effectuer un déni de service, au moyen d'un fichier malicieusement nommé accepté par la victime (CAN-2005-0573) ;
- une dernière vulnérabilité découverte dans le traitement de code HTML permet à un individu distant mal intentionné de réaliser un déni de service sur une application vulnérable, au moyen d'un code HTML malicieusement constitué (CAN-2005-0208).

## 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 1.1.4 :  
<http://gaim.sourceforge.net/security/index.php?id=12>
- Bulletin de sécurité de l'US-CERT VU#523888 du 21 février 2005 :  
<http://www.kb.cert.org/vuls/id/523888>
- Bulletin de sécurité de l'US-CERT VU#839280 du 21 février 2005 :  
<http://www.kb.cert.org/vuls/id/839280>
- Bulletin de sécurité Gentoo GLSA 200503-03 / Gaim du 1er mars 2005 :  
<http://www.gentoo.org/security/glsa/glsa-200503-03.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:049 du 04 mars 2005 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:049>
- Bulletin de sécurité RedHat RHSA-2005:215 du 10 mars 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-215.html>
- Mise à jour de sécurité du paquetage NetBSD gaim :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/chat/gaim/README.html>
- Référence CVE CAN-2005-0472 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0472>
- Référence CVE CAN-2005-0473 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0473>
- Référence CVE CAN-2005-0573 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0573>
- Référence CVE CAN-2005-0208 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0208>

## Gestion détaillée du document

**08 mars 2005** version initiale.

**11 mars 2005** ajout des références aux bulletins de sécurité RedHat et NetBSD.