



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 mai 2004  
N° CERTA-2004-AVI-017-003

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-2004-AVI-017>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2004-AVI-017-003   |
| Titre                       | Multiples vulnérabilités de GAIM   |
| Date de la première version | 29 janvier 2004  |
| Date de la dernière version | 13 mai 2004  |
| Source(s)                   | Bulletin de sécurité "12 x Gaim remote overflows" d'e-matters<br>Bulletin de sécurité MDKSA-2004:006 de Mandrake<br>Bulletin de sécurité GLSA 200401-04 de Gentoo<br>Bulletins de sécurité RHSA-2004:033 et RHSA-2004:032 de 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.

## 2 Systèmes affectés

GAIM versions 0.75 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités présentes dans le logiciel GAIM peuvent être exploitées par un utilisateur mal intentionné afin d'exécuter, à distance, du code arbitraire sur la plate-forme vulnérable.

## 4 Description

GAIM est un logiciel de messagerie instantanée compatible avec de nombreux logiciels de messagerie instantanée (AIM, MSN Messenger, ICQ, Yahoo messenger, Jabber, etc.).

De nombreuses vulnérabilités de type débordement de mémoire sont présentes dans GAIM. Un utilisateur mal intentionné peut, en exploitant une de ces vulnérabilités, exécuter à distance du code arbitraire sur la plate-forme vulnérable.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs :

- Correctif pour GAIM 0.75 :  
<http://gaim.sourceforge.net/gaim-0.75.patch>
- Bulletin de sécurité MDKSA-2004:006 de Mandrake :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:006>
- Bulletin de sécurité RHSA-2004:032 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-032.html>
- Bulletin de sécurité RHSA-2004:033 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-033.html>
- Bulletin de sécurité GLSA 200401-04 de Gentoo :  
<http://www.securityfocus.com/advisories/6277>
- Bulletin de sécurité SuSE-SA:2004:004 de SuSE :  
[http://www.suse.com/de/security/2004\\_04\\_gaim.html](http://www.suse.com/de/security/2004_04_gaim.html)
- Bulletin de sécurité DSA-434 de Debian :  
<http://www.debian.org/security/2004/dsa-434>
- Bulletin de sécurité FreeBSD du 12 février 2004 :  
<http://www.vuxml.org/freebsd>

## 6 Documentation

- GAIM :  
<http://gaim.sourceforge.net>
- Bulletin de sécurité "12 x Gaim remote overflows" d'e-matters :  
<http://security.e-matters.de/advisories/012004.txt>
- Référence CVE CAN-2004-0005 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0005>
- Référence CVE CAN-2004-0006 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0006>
- Référence CVE CAN-2004-0007 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0007>
- Référence CVE CAN-2004-0008 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0008>

## Gestion détaillée du document

**29 janvier 2004** version initiale.

**30 janvier 2004** ajout référence au bulletin de sécurité de SuSE.

**6 février 2004** ajout référence au bulletin de sécurité de Debian.

**13 mai 2004** ajout du bulletin de sécurité FreeBSD.