

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-2004-AVI-281>

---

### Gestion du document

Référence	CERTA-2004-AVI-281-002
Titre	Multiples vulnérabilités dans gaim
Date de la première version	30 août 2004
Date de la dernière version	08 septembre 2004
Source(s)	Bulletin de sécurité GLSA 200408-27 de Gentoo
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 0.81 et antérieures.

## 3 Résumé

De multiples vulnérabilités présentes dans gaim permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

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

De multiples vulnérabilités de type débordement de mémoire sont présentes dans gaim :

- CVE CAN-2004-0785 : vulnérabilités relatives à l'interprétation des messages au format rtf (Rich Text Format), à la résolution, via DNS, du nom de machine locale, à la réception d'URL de taille supérieure à 2048 caractères ;
- CVE CAN-2004-0754 : vulnérabilité liée à l'allocation mémoire lors de la réception d'un message habilement constitué envoyé par un serveur.

De plus, à l'installation de nouveaux "émoticons", gaim ne filtre pas correctement le nom du fichier archive (CVE CAN-2004-0784). Il est alors possible pour une personne mal intentionnée incitant l'utilisateur à installer une archive habilement constituée, d'exécuter des commandes au moyen de l'interpréteur de commandes lancé automatiquement par gaim pour l'installation de l'archive.

## 5 Solution

La version 0.82 de gaim corrige ces vulnérabilités.

## 6 Documentation

- Site internet de gaim :  
<http://gaim.sourceforge.net>
- Site internet de gaim, liste des vulnérabilités :  
<http://gaim.sourceforge.net/security>
- Bulletin de sécurité Gentoo GLSA-200408-27 du 27 août 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200408-27.xml>
- Bulletin de sécurité Red Hat RHSA-2004:400 du 7 septembre 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-400.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-2004-0754 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0754>
- Référence CVE CAN-2004-0784 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0784>
- Référence CVE CAN-2004-0785 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0785>

## Gestion détaillée du document

**30 août 2004** version initiale.

**01 septembre 2004** ajout de la référence au bulletin de sécurité NetBSD.

**08 septembre 2004** ajout de la référence au bulletin de sécurité de Red Hat.