



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2002
N° CERTA-2002-AVI-012

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans ICQ

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-2002-AVI-012>

Gestion du document

Référence	CERTA-2002-AVI-012
Titre	Débordement de mémoire dans ICQ
Date de la première version	25 janvier 2002
Date de la dernière version	–
Source(s)	Avis CA-2002-02 du CERT/CC
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.

2 Systèmes affectés

- Tous les systèmes Windows avec ICQ version 2001A ou antérieure ;
- Tous les systèmes Windows avec ICQ version antérieure à 2001B Beta v5.18 Build #3659 avec le module Voice Video & Games installé.

3 Résumé

Une vulnérabilité dans certaines versions d'ICQ permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine.

4 Description

ICQ est un outil qui permet l'échange de messages instantanés entre plusieurs utilisateurs distants. ICQ est très répandu sur les postes clients. Une vulnérabilité existe dans le client ICQ de Windows permettant l'exécution de code arbitraire par un utilisateur mal intentionné. Bien que certaines mesures aient été prises au niveau des serveurs ICQ, cette vulnérabilité demeure exploitable.

5 Contournement provisoire

Installer la version 2001B Beta v5.18 Build #3659. Celle-ci désinstalle le module Voice Video & Games. Bloquer au niveau du client ICQ les connexions directes provenant de n'importe quel client.

6 Solution

Il n'existe pas de correctif à ce jour.

7 Documentation

Avis du CERT/CC :

<http://www.cert.org/advisories/CA-2002-02.html>

<http://www.kb.cert.org/vuls/id/570167>

Bugtraq :

<http://www.securityfocus.com/bid/3813>

Sur le site d'ICQ :

<http://web.icq.com/help/quickhelp/1,,117,00.html>

Gestion détaillée du document

25 janvier 2002 version initiale.