

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du client IRC xchat

---

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-134>

---

### Gestion du document

Référence	CERTA-2004-AVI-134-004
Titre	Vulnérabilité du client IRC xchat
Date de la première version	19 avril 2004
Date de la dernière version	12 mai 2004
Source(s)	Message électronique de Peter Zelezny du 05 avril 2004 sur la liste de diffusion xchat-announce
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

xchat versions 1.8.0 (inclusive) à la version 2.0.8 (inclusive).

## 3 Résumé

Une vulnérabilité dans xchat permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

xchat est un client IRC (Internet Relay Chat) graphique. Dans le cas où xchat utilise un proxy SOCKS 5 contrôlé par un utilisateur mal intentionné, il est possible pour ce dernier de faire exécuter du code arbitraire à distance sur la plate-forme victime.

## 5 Contournement Provisoire

Ne pas utiliser de serveur proxy SOCKS 5 non digne de confiance.

## 6 Solution

Se référer au bulletin de sécurité fourni par l'éditeur (cf. Documentation).

## 7 Documentation

- Site Internet de xchat :  
<http://xchat.org>
- Message électronique de Peter Zelezny du 05 avril 2004 sur la liste de diffusion xchat-announce :  
<http://mail.nl.linux.org/xchat-announce/2004-04/msg00000.html>
- Avis de sécurité Secunia SA11409 du 19 avril 2004 :  
<http://secunia.com/advisories/11409/>
- Avis de sécurité Gentoo GLSA 200404-15 du 19 avril 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200404-15.xml>
- Avis de sécurité Debian DSA-493 du 21 avril 2004 :  
<http://www.debian.org/security/2004/dsa-493>
- Avis de sécurité Mandrake MDKSA-2004:036 du 21 avril 2004 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:036>
- Avis de sécurité Red Hat RHSA-2004:177 :  
<https://rhn.redhat.com/errata/RHSA-2004-177.html>
- Avis de sécurité FreeBSD du 23 avril 2004 :  
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité pour le paquetage NetBSD xchat :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>

## Gestion détaillée du document

**19 avril 2004** version initiale.

**21 avril 2004** ajout de l'avis de sécurité Debian.

**22 avril 2004** ajout de l'avis de sécurité Mandrake.

**30 avril 2004** ajout de l'avis de sécurité Red Hat.

**12 mai 2004** ajout des références aux bulletins de sécurité FreeBSD et NetBSD.