

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Trillian

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-2008-AVI-266>

Gestion du document

Référence	CERTA-2008-AVI-266
Titre	Vulnérabilités dans Trillian
Date de la première version	22 mai 2008
Date de la dernière version	–
Source(s)	–
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

Trillian versions antérieures à 3.1.10.0.

3 Résumé

Trois vulnérabilités de *Trillian* permettent l'exécution de code arbitraire à distance.

4 Description

Trillian est un client de messagerie instantanée multi-protocoles capable notamment de gérer les conversations ICQ, AIM, Jabber, MSN, Yahoo et IRC.

Trois vulnérabilités ont été découvertes dans ce produit :

- un débordement de mémoire lors du traitement des entêtes de paquets MSN permet d'exécuter du code arbitraire à distance ;

- une erreur lors du traitement des fichiers XML permet d'exécuter du code arbitraire à distance ;
- un débordement de mémoire lors du traitement des balises FONT permet, par le biais d'un fichier image, d'exécuter du code arbitraire à distance.

5 Solution

Mettre *Trillian* à jour en version 3.1.10.0 (voir Documentation).

6 Documentation

- Site de téléchargement de la dernière version de *Trillian* :
<http://www.ceruleanstudios.com/learn/>

Gestion détaillée du document

22 mai 2008 version initiale.