



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 février 2004
N° CERTA-2004-AVI-048

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur 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-2004-AVI-048>

Gestion du document

Référence	CERTA-2004-AVI-048
Titre	Vulnérabilités sur Trillian
Date de la première version	26 février 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Ematters O22004
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

- Déni de service ;
- exécution de code arbitraire ;

2 Systèmes affectés

- Trillian 0.x ;
- Trillian Pro 1.x ;
- Trillian Pro 2.x ;
- Trillian 0.71 à 0.74F.

3 Résumé

Deux vulnérabilités ont été découvertes sur le logiciel de messagerie instantanée qui permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire, via un paquet malicieusement construit, sur le système vulnérable.

4 Description

Trillian est un logiciel de messagerie instantanée assez répandu sous Windows.

La première vulnérabilité est présente dans la gestion du protocole AIM/Oscar : un débordement de mémoire présent dans l'allocation de la mémoire pour les paquets DirectIM permet à un utilisateur mal intentionné de réaliser un déni de service ou l'exécution d'un code arbitraire sur le système vulnérable.

La seconde vulnérabilité est présente dans l'analyse d'un paquet YMSG : un nom de clef malicieusement construit peut entraîner l'exécution de code arbitraire. L'exploitation de cette vulnérabilité nécessite la possibilité de conduire une attaque de type « homme du milieu ».

5 Solution

Mettre à jour ou réinstaller la version 0.74G de Trillian ou la version 2.011 de Trillian Pro (cf section documentation).

6 Documentation

- Les correctifs et nouvelles versions sont disponibles à cette adresse :
<http://www.trillian.cc/downloads/>
- Avis de sécurité de Ematters :
<http://security.e-matters.de/advisories/022004.html>

Gestion détaillée du document

26 février 2004 version initiale.