

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités Skype

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-2005-AVI-423>

Gestion du document

Référence	CERTA-2005-AVI-423
Titre	Vulnérabilités Skype
Date de la première version	26 octobre 2005
Date de la dernière version	–
Source(s)	Avis SKYPE-SB/2005-002 Avis SKYPE-SB/2005-003
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 à distance de commandes arbitraires ;
- déni de service.

2 Systèmes affectés

Toutes les plateformes et toutes les versions pour la vulnérabilité sur le débordement de variable dans le tas.
Le problème affecte les versions de SKYPE pour Windows dont les versions sont comprises entre 1.1.*.0 et 1.4.*.83 incluses pour la vulnérabilité sur les VCARDs et les URIs.

3 Description

SKYPE est un logiciel de téléphonie sur IP. Deux vulnérabilités affectent ce logiciel.

Un première vulnérabilité est liée à la gestion des URI et de l'importation des VCARDs. Un utilisateur mal intentionné peut construire des URLS astucieusement formées dans le but de produire un débordement de variable pouvant conduire à l'exécution de code arbitraire.

Une seconde vulnérabilité qui met en œuvre un débordement de variable dans le tas permet de produire un arrêt brutal du logiciel (déni de service). Cette vulnérabilité est accessible à un utilisateur distant qui peut envoyer un flux réseau astucieusement construit.

4 Contournement provisoire

Par nature, ce type d'application se prête au mal au filtrage sur des pare-feus (voir note CERTA-2001-INF-003).

5 Solution

Appliquer les correctifs du vendeur.

6 Documentation

- Avis SKYPE :
 - <http://www.skype.com/security/skype-sb-2005-02.html>
 - <http://www.skype.com/security/skype-sb-2005-03.html>
- note d'information du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003>

Gestion détaillée du document

26 octobre 2005 version initiale.