

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans TANDBERG MXP

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-2009-ALE-022>

Gestion du document

Référence	CERTA-2009-ALE-022
Titre	Vulnérabilité dans TANDBERG MXP
Date de la première version	11 décembre 2009
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

Déni de service à distance.

2 Systèmes affectés

La vulnérabilité a été confirmée sur les produits TANDBERG MXP, versions F8.2, F8.0, F7.2 et F6.3.

3 Résumé

Une vulnérabilité affecte les produits TANDBERG MXP lors du traitement du flux H. 225 RAS (*Registration, Administration and Status*). Elle permet à une personne malveillante distante de provoquer un déni de service.

4 Description

Une vulnérabilité affecte les produits TANDBERG MXP lors du traitement du flux H. 225 RAS. Une personne malveillante distante peut l'exploiter au moyen d'un nombre déterminé de paquets identiques afin d'épuiser les ressources et ainsi provoquer un déni de service.

Il n'est pas exclu que la vulnérabilité puisse conduire à une attaque autre que le déni de service.

5 Contournement provisoire

En attendant la mise à disposition d'un correctif, le CERTA recommande :

- de maîtriser le réseau afin de n'autoriser des connexions qu'avec des correspondants connus ;
- de surveiller le réseau afin de détecter un trafic inhabituel ;
- d'utiliser un produit alternatif.

6 Documentation

Gestion détaillée du document

11 décembre 2009 version initiale.