Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2007
N° CERTA-2007-AVI-506

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Alcatel OmniPCX Enterprise Communication Server

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-2007-AVI-506

Gestion du document

Référence	CERTA-2007-AVI-506
Titre	Vulnérabilité dans Alcatel OmniPCX Enterprise Communication Server
Date de la première version	21 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Alcatel-Lucent PSIRT du 14 novembre 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Alcatel-Lucent OmniPCX Enterprise R7.1 ;
- Alcatel-Lucent OmniPCX Enterprise R7.0 ;
- Alcatel-Lucent OmniPCX Enterprise R6.2 ;
- Alcatel-Lucent OmniPCX Enterprise R6.1 ;
- Alcatel-Lucent OmniPCX Enterprise R6.0 ainsi que les versions précédentes.

3 Résumé

Une vulnérabilité a été identifiée dans les passerelles de téléphonie (PABX ou *Private Automatic Branch Exchange*) Alcatel-Lucent OmniPCX Enterprise. Elle permettrait à une personne malveillante pouvant correspondre avec ce système de détourner les flux audio à destination d'un poste. Cette attaque peut également servir pour se mettre en entredeux (man-in-the-middle) d'une conversation.

4 Description

Une vulnérabilité a été identifiée dans les passerelles de téléphonie (PABX ou *Private Automatic Branch Exchange*) Alcatel-Lucent OmniPCX Enterprise.

Une personne malveillante pourrait forger une requête TFTP particulière en usurpant l'identité (adresse MAC) d'un poste terminal. L'interprétation de cette trame impliquerait au PABX de router certains flux audio destinés initalement au terminal vers le poste malveillant.

Cette attaque peut également servir pour se mettre en entredeux (man-in-the-middle) d'une conversation.

5 Solution

Se référer au bulletin de sécurité de l'éditeur Alcatel-Lucent pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Annonce publique du PSIRT Alcatel-Lucent du 14 novembre 2007 :
  http://www1.alcatel-lucent.com/psirt/statements/2007004/IPTouchDOS.htm
- Liste des annonces de sécurité PSIRT Alcatel-Lucent :
  http://www1.alcatel-lucent.com/psirt/statements.htm
- Référence CVE CVE-2007-5361 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5361

Gestion détaillée du document

21 novembre 2007 version initiale.