

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de OmniPCX Entreprise

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-406>

Gestion du document

Référence	CERTA-2007-AVI-406
Titre	Vulnérabilité de OmniPCX Entreprise
Date de la première version	18 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin Alcatel-Lucent du 11 septembre 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

- Exécution de code arbitraire à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

OmniPCX entreprise, jusqu'à la version R7.1 comprise.

3 Résumé

Une vulnérabilité dans l'outil de maintenance d'OmniPCX entreprise permet à utilisateur malintentionné de réaliser :

- une exécution de code arbitraire à distance ;
- une atteinte à l'intégrité des données ;
- une atteinte à la confidentialité des données.

4 Description

L'outil de maintenance d'OmniPCX Entreprise a une interface web. Un script CGI ne filtre pas correctement les données entrées. Cette insuffisance de filtrage peut servir à exécuter des commandes sur le système vulnérable avec les droits du serveur web. Cette vulnérabilité permet à utilisateur malintentionné de réaliser :

- une exécution de code arbitraire à distance ;
- une atteinte à l'intégrité des données ;
- une atteinte à la confidentialité des données.

5 Solution

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

6 Documentation

- Bulletin de sécurité *Alcatel-Lucent* du 11 septembre 2007 :
<http://www1.alcatel-lucent.com/psirt/statements/2007002/OXEUMT.htm>
- Référence CVE CVE-2007-3010 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3010>

Gestion détaillée du document

18 septembre 2007 version initiale.