

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Alcatel OmniPCX Office

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-2008-AVI-260>

Gestion du document

Référence	CERTA-2008-AVI-260
Titre	Vulnérabilité dans Alcatel OmniPCX Office
Date de la première version	22 mai 2008
Date de la dernière version	–
Source(s)	Avis de sécurité PSIRT Alcatel-Lucent et DSECRG-08-020
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Les versions d'Alcatel-Lucent OmniPCX Office :

- OXO210 antérieures à 210/091.001 ;
- OX0310 antérieures à 310/056.001 ;
- OX0410 antérieures à 410/057.001 ;
- OX0510 antérieures à 510/037.001 ;
- OX0600 antérieures à 610/014.001.

3 Résumé

Une vulnérabilité a été identifiée dans un script CGI associé à l'interface Web d'Alcatel-Lucent OmniPCX Office. Celle-ci peut être exploitée par une personne distante pour exécuter des commandes arbitraires sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans un script CGI associé à l'interface Web d'Alcatel-Lucent OmniPCX Office. Elle implique */cgi-data/FastJSData.cgi*.

Cette vulnérabilité peut être exploitée par une personne distante pour exécuter des commandes arbitraires sur le système vulnérable.

5 Solution

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

6 Documentation

- Référence CVE CVE-2008-1331 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1331>
- Mises à jour fournies par Alcatel-Lucent :
http://www1.alcatel-lucent.com/enterprise/en/products/ip_telephony/omnipcxenterprise/index.html
- Avis de sécurité Alcatel Lucent SA034 :
<http://www1.alcatel-lucent.com/psirt/statements/2008001/OXOrexe.htm>

Gestion détaillée du document

22 mai 2008 version initiale.