

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des produits Alcatel-Lucent OmniVista 4760

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-2010-AVI-453>

Gestion du document

Référence	CERTA-2010-AVI-453
Titre	Vulnérabilité des produits Alcatel-Lucent OmniVista 4760
Date de la première version	23 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Alcatel-Lucent 201002 du 20 septembre 2010
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 ;
- déni de service à distance.

2 Systèmes affectés

Alcatel-Lucent OmniVista 4760.

3 Résumé

Une vulnérabilité présente dans la suite logiciel OmniVista 4760 de Alcatel-Lucent permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Le serveur mandataire (*proxy*) inclus dans la suite logiciel OmniVista 4760 de Alcatel-Lucent présente une faille de type débordement de mémoire. Elle permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire par le biais d'une requête HTTP construite de façon particulière.

5 Solution

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

6 Documentation

- Site de Alcatel-Lucent :
<http://www.alcatel-lucent.com>
- Bulletin de sécurité Alcatel-Lucent 201002 du 20 septembre 2010 :
http://www.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Corporate&LMSG_CONTENT_FILE=Support/Security/2010002.pdf
- Référence CVE CVE-2010-3281 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3281>

Gestion détaillée du document

23 septembre 2010 version initiale.