

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'Alcatel OmniSwitch

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-415>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2008-AVI-415 |
| Titre | Vulnérabilité d'Alcatel OmniSwitch |
| Date de la première version | 14 août 2008 |
| Date de la dernière version | - |
| Source(s) | Bulletin de sécurité Alcatel-Lucent PR 122812 du 06 août 2008 |
| 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.

2 Systèmes affectés

Alcatel-Lucent OmniSwitch, séries :

- OS 6600 ;
- OS 6800 ;
- OS 6850 ;
- OS 7000 ;
- OS 9000.

3 Résumé

Une vulnérabilité dans OmniSwitch d'Alcatel-Lucent permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Les produits OmniSwitch d'Alcatel-Lucent contiennent un serveur web embarqué pour leur administration. Un défaut de vérification de bornes lors de la réception de requêtes GET avec *cookies* permet à un utilisateur malveillant de provoquer un débordement de mémoire. L'exploitation de cette vulnérabilité permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

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 PR 122812 du 06 août 2008 :
<http://www1.alcatel-lucent.com/psirt/statements/2008002/OmniSwitch.htm>

Gestion détaillée du document

14 août 2008 version initiale.