Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 mars 2002
N° CERTA-2002-AVI-060

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le commutateur Alteon ACEdirector (AD) de Nortel Networks

Gestion du document

Référence	CERTA-2002-AVI-060
Titre	Vulnérabilité dans le commutateur Alteon ACEdirector (AD) de Nortel Networks
Date de la première version	25 mars 2002
Date de la dernière version	–
Source(s)	Base de vulnérabilités BugTraq
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

Divulgation de données.

2 Systèmes affectés

Les équipements de la gamme Alteon ACEdirector (AD) de Nortel Networks.

3 Résumé

Une vulnérabilité dans les équipements Alteon ACEdirector (AD) permet la divulgation de l'adresse IP réelle des serveurs Web gérés par ces équipements.

4 Description

Alteon ACEdirector (AD) de Nortel Networks est un équipement, communément appelé *commutateur de niveau 7*, dont le rôle est de gérer du trafic Web pour plusieurs serveurs (répartition de charge, redirection en fonction de l'application ou de l'URL, etc...).

Lorsque l'équipement fonctionne en mode «répartition de charge» entre les différents serveurs Web, la fonctionalité est normalement transparente pour le client qui ne connait qu'une adresse IP (appelée adresse IP virtuelle de l'équipement).

Cependant, une vulnérabilité dans la gestion des fermeture de session TCP d'Alteon ACEdirector permet d'être en communication directe avec un serveur et de connaître ainsi son adresse IP.

5 Solution

Nortel Networks distribue des mises à jour du système d'exploitation ne permettant plus l'exploitation de cette vulnérabilité :

- WebOS 8.3.24.5 pour les versions 8.3.x ;
- WebOS 9.0.41.5 pour les versions 9.x ;
- WebOS 10.0.25.1 pour les versions 10.x

Des correctifs sont en cours d'élaboration pour les versions 8.0 et 8.1. Aucun correctif n'est en revanche prévu pour des versions plus anciennes de WebOS.

6 Documentation

Archive de securityfocus (Bugtraq) :
http://online.securityfocus.com/bid/3964 .

Gestion détaillée du document

25 mars 2002 version initiale.