Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 avril 2001
N° CERTA-2001-ALE-005

**Affaire suivie par :**
CERTA

# BULLETIN D'ALERTE DU CERTA

## Objet : Vulnérabilités dans les modems ADSL d'Alcatel



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2001-ALE-005 |
| Titre | Vulnérabilités dans les modems ADSL d'Alcatel |
| Date de la première version | 11 avril 2001 |
| Date de la dernière version | – |
| Source(s) | Avis CA-2001-08 du CERT/CC<br>Avis du San Diego Supercomputer Center |
| Pièce(s) jointe(s) | Aucune |

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Modification et accès à la configuration courante (y compris les mots de passe),
- Déni de service, avec un éventuel retour constructeur nécessaire,
- Destruction ou implantation de code malicieux dans le logiciel du modem.

## 2 Systèmes affectés

Il a été établi que les modems ADSL suivants sont concernés :

- Alcatel Speed TouchTM Home
- Alcatel A 1000

## 3 Résumé

Les modems Alcatel sont couramment loués ou vendus dans le cadre des offres de connexion ADSL des FAIs. Ces modems possèdent un système d'exploitation aux fonctionnalités semblables aux systèmes Unix classiques. Ils offrent entre autres un certain nombre de services IP (http, telnet, ftp, tftp) permettant la mise à jour et l'administration du modem.

Une mauvaise protection de l'accès à ces services permet à un utilisateur mal intentionné de prendre le contrôle du modem depuis le réseau local désservi par le modem (LAN).

# 4 Description

## 4.1 Accès TFTP

Les 2 modèles sont accessibles par le protocole tftp (69/udp), sans aucune authentification, depuis le réseau LAN. Il est possible par ce biais de modifier la configuration ou le logiciel du modem. Ce risque peut s'étendre à un individu malveillant connecté via internet si il parvient à compromettre ou à utiliser comme rebond (envois de paquets sur le port echo - 7udp -,... ) une machine présente sur le LAN.

## 4.2 Mots de passe par défaut

Les services http et ftp, ainsi que telnet pour le seul modèle Speed Touch, sont accessibles sans aucun mot de passe par défaut. Ce défaut ne peut être corrigé sur le modèle A 1000, et doit l'être par l'utilisateur dans l'autre cas. Cependant, il arrive que le FAI prenne la précaution d'en rajouter un.

## 4.3 Compte d'administration expert

Malgré l'éventuelle mise en place d'un mot de passe utilisateur, il existe un compte privilégié, dénommé "expert" . Son mot de passe n'est pas modifiable, mais dépend uniquement de l'adresse MAC du matériel et de la version logicielle du modem via un principe de challenge/réponse. Il existe, en libre accès sur le net, un générateur de mot de passe à partir du challenge qui a démontré son efficacité pour de nombreuses configurations.

# 5 Solution

- Pour la version Speed Touch, il est recommandé de mettre un mot de passe d'accès dès la mise en service si le fournisseur d'accès ne l'a pas fait (pour le le modèle A 1000 aucun mot de passe ne peut être imposé pour les services ftp et http, et telnet est restreint à l'utilisateur "expert"). Cependant, les vulnérabilités sur le compte "expert" et l'accès tftp ne sont pas pour autant levées.
- Restreindre l'accès aux services (tftp, telnet, ftp et http) du modem depuis le LAN à une ou quelques machines d'administration à l'aide d'un garde-barrière ou d'un routeur filtrant entre le modem et le réseau LAN.
- Mettre en place un filtre (routeur, garde-barrière) entre l'internet et le réseau local pour éviter les rebonds (utiliser un garde-barrière "personnel" pour une machine unique) :
  - pas d'adresse IP source appartenant au LAN arrivant sur l'interface externe,
  - pas d'adresse IP source avec une adresse de "broadcast",
  - bloquer l'accès au port udp echo (7/udp) vers le réseau interne.

# 6 Documentation

- Avis du CERT/CC :
  http://www.cert.org/advisories/CA-2001-08.html
- Avis du San Diego Supercomputer Center :
  http://security.sdsc.edu/self-help/alcatel
- Communiqué d'Alcatel :
  http://www.alcatel.com/consumer/dsl/security.htm

# Gestion détaillée du document

**11 avril 2001** version initiale.