Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 février 2002
N° CERTA-2002-ALE-005

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Risque de compromission des auto-commutateurs (PABX) ALCATEL 4400

Gestion du document

Référence	CERTA-2002-ALE-005
Titre	Risque de compromission des auto-commutateurs (PABX) ALCATEL 4400
Date de la première version	20 février 2002
Date de la dernière version	–
Source(s)	Avis de sécurité "Playing around with ALCATEL 4400 PBX" de Securitybugware
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

- Accès non autorisé ;
- altération des données.

2 Systèmes affectés

L'ensemble des auto-commutateurs ALCATEL de la série 4400.

3 Résumé

Un message récemment posté sur Internet donne la liste des mots-de-passe par défaut qui protègent les comptes des auto-commutateurs ALCATEL 4400.

Si l'auto-commutateur est connecté à un modem ou à un réseau local, il y a un risque de compromission et de modification du paramétrage.

4 Description

Les auto-commutateurs ALCATEL 4400 utilisent le système temps-réel Chorus.
Lors de l'installation, vingt comptes sont créés :

- 4 comptes verrouillés (sur lesquels il est impossible de se connecter) : `daemon`, `bin`, `sys`, `adm`.
- 13 comptes avec un mot de passe : `install`, `halt`, `dhs3pms`, `adfexc`, `client`, `kermit`, `dhs3mt`, `at4400`, `mtch`, `mtcl`, `root`, `nmcmao`, `mntple`.
- 1 compte sans mot-de-passe qui ne permet que l'exécution d'une commande : `sync`.
- 2 comptes sans aucun mot-de-passe : `swinst`, `pcmao`.

Un message récemment posté sur Internet donne la liste des mots-de-passe par défaut de onze de ces comptes.

5 Solution

Vérifier qu'à la suite de l'installation de l'Alcatel 4400, les mots-de-passe ont bien été changés. Sinon :

- modifier de toute urgence les mots-de-passe des 13 comptes (cf. section Description);
- mettre un mot-de-passe sur les 2 comptes qui n'en possèdent pas.

6 Documentation

Avis de sécurité "Playing around with ALCATEL 4400 PBX" de Securitybugware :
http://www.securitybugware.org/Other/5097.html

Gestion détaillée du document

20 février 2002 version initiale.