Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 mars 2005
N° CERTA-2005-AVI-113

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits Avaya

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-2005-AVI-113

Gestion du document

Référence	CERTA-2005-AVI-113
Titre	Vulnérabilité dans les produits Avaya
Date de la première version	14 mars 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya du 02 mars 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

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

1 Risque

Atteinte à la confidentialité des données.

2 Systèmes affectés

Toutes les versions des produits cités ci-dessous sont affectées :

- Avaya CMS Supervisor ;
- Avaya Conversant / Interactive Voice Response ;
- Avaya Interactive Response 1.x ;
- Avaya IP Agent 4.x ;
- Avaya IP Office 2.x ;
- IP Softphone 5.x ;
- Softconsole 1.x.

3 Résumé

De nombreux produits Avaya sont vulnérables à des attaques pouvant permettre à un utilisateur mal intentionné de porter atteinte à la confidentialité des données présentes sur le système vulnérable.

4 Description

La vulnérabilité est causée par des sauvegardes d'informations sensibles non sécurisées permettant à une personne malveillante ayant un accès local au système de porter atteinte à la confidentialité des données présentes sur le système.

5 Solution

L'éditeur recommande pour tous les produits affectés de :

– limiter l'accès au système et aux clés de registre.

Concernant les produits Avaya suivant :

– IP Softphone ;
– IP Agent ;
– IP Softconsole.

l'éditeur Avaya recommande de :

– ne pas utiliser l'option "Se souvenir du mot de passe pour les prochaines sessions"

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

6 Documentation

– Bulletin de sécurité Avaya du 02 mars 2005 :
  http://support.avaya.com/elmodocs2/security/ASA-2005-41_Sensitive_Info_Leak.pdf
– Référence CVE CAN-2005-0506 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0506

Gestion détaillée du document

14 mars 2005 version initiale.