

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Avaya IP Office Manager

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-2011-AVI-363>

Gestion du document

Référence	CERTA-2011-AVI-363
Titre	Vulnérabilité dans Avaya IP Office Manager
Date de la première version	17 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Avaya ASA-2011-156 du 15 juin 2011
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Avaya B5800 Branch Gateway 6.x ;
- Avaya IP Office toutes versions.

3 Résumé

Une vulnérabilité découverte dans les produits Avaya permet, sous certaines conditions, un accès illégitime aux données présentes sur le serveur hébergeant cette solution.

4 Description

Un serveur TFTP vulnérable est présent dans les solutions Avaya B5800 Branch Gateway 6.X et Avaya IP Office. Un utilisateur malveillant sur le réseau local peut, sous certaines conditions, accéder de façon illégitime aux données présentes sur le serveur sur lequel cette solution est installée.

5 Solution

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

6 Documentation

- Bulletin de sécurité Avaya ASA-2011-156 du 15 juin 2011 :
<https://support.avaya.com/css/P8/documents/100141179>

Gestion détaillée du document

17 juin 2011 version initiale.