

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Cisco Secure Desktop

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-2006-AVI-484>

Gestion du document

Référence	CERTA-2006-AVI-484
Titre	Multiples vulnérabilités de Cisco Secure Desktop
Date de la première version	09 novembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco du 08 novembre 2006
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 ;
- élévation de privilèges.

2 Systèmes affectés

La version 3.1.1.33 de Cisco Secure Desktop (CSD), ainsi que celles antérieures.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le produit Cisco Secure Desktop. Une personne malveillante pourrait exploiter celles-ci, afin de récupérer de l'information à l'insu de l'utilisateur, de contourner la politique de sécurité, voire d'acquiescer les mêmes droits que ceux de l'administrateur.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le produit Cisco Secure Desktop. Parmi celles-ci :

- il y aurait une mauvaise gestion des fichiers lorsque le navigateur Internet qui affiche une page d'accueil s'ouvre après une session SSL VPN. Ceux-ci, pouvant être des fichiers temporaires, un historique, ou des cookies pourraient être récupérés en clair à la fin de la session chiffrée.
- le passage d'un bureau sécurisé (*Secure Desktop*) à un bureau standard (*Local Desktop*) ne serait pas correctement contrôlé. Une personne pourrait donc contourner l'option de configuration choisie.
- les fichiers d'installation de Cisco Secure Desktop n'auraient pas des droits adaptés. Cette vulnérabilité, exploitée par une personne malveillante locale, lui permettrait de contourner la politique de sécurité en élevant ses privilèges.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 72020 du 08 novembre 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20061108-csd.shtml>
- Avis de sécurité de iDefense Labs du 08 novembre 2006 :
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=442>

Gestion détaillée du document

09 novembre 2006 version initiale.