

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des concentrateurs Cisco VPN 3000

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-2002-AVI-199>

Gestion du document

Référence	CERTA-2002-AVI-199
Titre	Multiples vulnérabilités des concentrateurs Cisco VPN 3000
Date de la première version	04 septembre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco
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

- Déni de service ;
- divulgation d'informations sensibles (y compris des mots de passe) ;
- élévation de privilèges.

2 Systèmes affectés

Concentrateurs Cisco VPN 3000 et clients VPN 3002.

3 Résumé

De multiples vulnérabilités ont été découvertes sur les concentrateurs Cisco VPN 3000.

4 Description

Les concentrateurs Cisco VPN 3000 servent à établir des Réseaux Privés Virtuels pour des communications chiffrées et authentifiées.

Le numéro des vulnérabilités ci-dessous correspond à l'identification Cisco :

- CSCdt56514 : une vulnérabilité du processus d'authentification permet un accès non autorisé au réseau protégé par le concentrateur Cisco VPN 3000 ;
- CSCdu15622 : une URL habilement construite envoyée à l'interface HTML du VPN 3000 peut provoquer un déni de service ;
- CSCdu35577 : les bannières de plusieurs applications donnent des d'informations qui ne devraient pas être révélées ;
- CSCdu82823 : le démon telnet est vulnérable à un débordement de mémoire ,
- CSCdv66718 : le client natif PPTP de Windows peut provoquer le redémarrage du concentrateur ;
- CSCdv88230 et CSCdw22408 : les mots de passe des utilisateurs peuvent être vus en clair via une page HTML ;
- CSCdw50657 : les mots de passe des certificats peuvent être vus en clair via une page HTML ;
- CSCdx07754 : une vulnérabilité du filtre XML permet un accès non autorisé au réseau protégé par le concentrateur ;
- CSCdx24622 : l'accès à certaines pages HTML est autorisé sans authentification préalable ;
- CSCdx24632 : une vulnérabilité de l'interface HTML permet de provoquer un déni de service ;
- CSCdx39981 : une vulnérabilité dans le traitement de la chaîne de caractères correspondant au nom d'utilisateur peut provoquer un déni de service ;
- CSCdx54675 : une mauvaise gestion des tunnels IPSec peut provoquer la coupure d'une connexion établie ;
- CSCdy38035 : une vulnérabilité dans le traitement des paquets ISAKMP peut provoquer un déni de service.

5 Contournement provisoire

Certaines vulnérabilités peuvent être contournées en n'autorisant l'accès à l'interface HTML que depuis une source sûre.

Se reporter à l'avis Cisco pour plus de détails.

6 Solution

Les versions du firmware 3.5.5 et 3.6.1 corrigent ces vulnérabilités.

7 Documentation

Avis de sécurité Cisco :

<http://www.cisco.com/warp/public/707/vpn3K-multiple-vuln-pub.shtml>

Gestion détaillée du document

04 septembre 2002 version initiale.