Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 août 2002
N° CERTA-2002-AVI-169

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur VPN 5000 de CISCO

Gestion du document

Référence	CERTA-2002-AVI-169
Titre	Vulnérabilité sur VPN 5000 de CISCO
Date de la première version	08 août 2002
Date de la dernière version	–
Source(s)	Bulletin 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

Divulgation d'informations.

2 Systèmes affectés

- les séries des équipements VPN 5000 de CISCO ayant pour logiciel les versions 6.0.21.0002 et 5.2.23.0003 (les modèles VPN 5001, VPN 5002, VPN 5008 sont concernés par cette vulnérabilité) ;
- les séries des équipements IntraPort (IntraPort 2, Intraport 2+, IntraPort Enterprise-2 IntraPort Entreprise-8, IntraPort Carrier-2 et IntraPort Carrier-8).

3 Résumé

Une vulnérabilité est présente sur les équipements CISCO cités ci-dessus quand ils sont configurés pour utiliser le protocole d'authentification RADIUS. Cette vulnérabilité permet à un utilisateur mal intentionné de récupérer les mots de passes non chiffrés envoyés dans une requête lors de réémission vers un serveur RADIUS.

4 Description

Le service RADIUS est un service qui permet l'authentification des utilisateurs. Une vulnérabilité est présente sur les équipements CISCO cités ci-dessus lorsque ce service est utilisé avec les protocoles d'authentifications PAP ou Challenge.

Pour authentifier l'utilisateur, les équipements VPN 5000 utilisent une base de données interne ou un serveur RADIUS.

Lors de l'utilisation d'un serveur RADIUS, une requête contenant le mot de passe chiffré de l'utilisateur désirant se connecter est envoyée depuis l'équipement CISCO vers le serveur RADIUS.

La vulnérabilité présente sur les VPN 5000 apparaît si le serveur RADIUS n'a pas répondu à cette requête. Dans ce cas, une seconde requête, contenant cette fois le mot de passe « non chiffré » de l'utilisateur est envoyée au serveur. Cette vulnérabilité permet à un utilisateur mal intentionné de récupérer le mot de passe transmis dans cette requête.

5 Contournement provisoire

Dans l'attente d'appliquer le correctif il est possible d'utiliser le protocole d'authentification CHAP :
Dans la section RADIUS mettre ChallengeType = CHAP

6 Solution

Appliquer le correctif correspondant à la version de votre logiciel (cf section documentation).

7 Documentation

- Bulletin de sécurité CISCO :
  http://www.cisco.com/warp/public/707/vpn5k-radius-pap-vuln-pub.shtml
- Correctifs disponibles sur le site de CISCO à l'adresse :
  http://www.cisco.com/public/sw-center/

Gestion détaillée du document

08 août 2002 version initiale.