

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CISCOSecure sous Windows NT Server

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-2000-AVI-051>

Gestion du document

Référence	CERTA-2000-AVI-051
Titre	Vulnérabilités dans CISCOSecure sous Windows NT Server
Date de la première version	22 septembre 2000
Date de la dernière version	–
Source(s)	Cisco Security Advisory
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 des mécanismes d'authentification ;
- Déni de service ;
- Exécution de code arbitraire.

2 Systèmes affectés

CiscoSecure Acces Control Server pour Windows NT versions 2.4 (2) et antérieures.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le produit CiscoSecure.
Elles permettent à une personne mal intentionnée de :

- Provoquer une erreur fatale dans le module CSCAdmin ;
- Placer CiscoSecure ASC dans un état instable ;
- de contourner les mécanismes d'authentification lorsque CiscoSecure ACS est utilisé avec un serveur LDAP.

4 Description

Le logiciel CiscoSecure ACS est utilisé comme serveur de contrôle d'accès pour définir les accès aux réseaux et les services pouvant être autorisés.

Trois vulnérabilités ont été découvertes :

- Le module CSAdmin ne vérifie pas correctement certaines variables d'environnement. Un utilisateur mal intentionné peut fabriquer une URL malformée provoquant ainsi un débordement de pile. Ce débordement peut soit provoquer un « plantage » du module CSAdmin ou exécuter du code arbitraire.
- CiscoSecure ACS utilise TACACS+ afin de gérer l'authentification des utilisateur. Un utilisateur mal intentionné peut, par le biais d'un paquet TACACS+ malformé, mettre le logiciel dans un état instable.
- Lors de l'utilisation de CiscoSecure ACS avec un annuaire LDAP autorisant l'absence de mot de passe, un utilisateur mal intentionné peut contourner les mécanismes d'authentification afin d'obtenir des privilèges sur un routeur ou un commutateur.

Nota : La version unix n'est pas concernée par ces vulnérabilités

5 Solution

Télécharger la version 2.4 (3) de CiscoSecure ACS :

<http://www.cisco.com>

6 Documentation

Avis de sécurité Cisco :

<http://www.cisco.com/warp/public/707/csecureacsnt-pub.shtml>

Gestion détaillée du document

22 septembre 2000 version initiale.