

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les commutateurs 3Com 4500G

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-2009-AVI-113>

Gestion du document

Référence	CERTA-2009-AVI-113
Titre	Vulnérabilité dans les commutateurs 3Com 4500G
Date de la première version	25 mars 2009
Date de la dernière version	–
Source(s)	Notes de version 3Com s3q05_02_00s56(s168) du 25 février 2009
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.

2 Systèmes affectés

Commutateurs 3Com 4500G en version s3q05_01_03s56(s168).

3 Résumé

Une vulnérabilité dans les commutateurs 3Com 4500G permet de contourner le mécanisme d'authentification.

4 Description

Une vulnérabilité a été découverte dans les commutateurs (*switch*) 3Com 4500G configurés de telle sorte que l'authentification par TACACS soit permise pour les utilisateurs SSH. Dans ce cas, un utilisateur SFTP peut accéder au commutateur sans passer par l'étape d'authentification.

5 Solution

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

6 Documentation

– Notes de version 3Com s3q05_02_00s56(s168) du 25 février 2009 :

[http://support.3com.com/documents/switches/4500G/Switch%204500G%20s3q05_02_00s56\(s168\)%20Release%20Notes.pdf](http://support.3com.com/documents/switches/4500G/Switch%204500G%20s3q05_02_00s56(s168)%20Release%20Notes.pdf)

Gestion détaillée du document

25 mars 2009 version initiale.