

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits 3Com SuperStack 3 Switch 4400

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-493>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2006-AVI-493 |
| Titre | Vulnérabilité dans les produits 3Com SuperStack 3 Switch 4400 |
| Date de la première version | 14 novembre 2006 |
| Date de la dernière version | – |
| Source(s) | Avis de sécurité 3Com 3COM-06-004 du 19 octobre 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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- 3Com SuperStack 3 Switch 4400 ;
- 3Com SuperStack 3 Switch 4400PWR ;
- 3Com SuperStack 3 Switch 4400SE ;
- 3Com SuperStack 3 Switch 4400FW.

Les logiciels des matériels ayant une version antérieure ou égale à 5.11, 6.00 ou 6.10 seraient vulnérables.

3 Description

Une vulnérabilité a été identifiée dans les produits 3Com de la famille des SuperStack 3 (SS3) 4400 Switch. Il s'agirait d'une mauvaise manipulation de certains paquets liés à la gestion du système. Une personne créant de tels paquets et pouvant les adresser au système dans le VLAN de gestion, pourrait accéder à des informations de configuration, comme la chaîne de caractères *community string* de SNMP. Connaissant cette dernière, il pourrait

alors effectuer un ensemble d'opérations sur le système vulnérable, tels désactiver des ports ou reconfigurer les VLANs.

4 Solution

Se référer au bulletin de sécurité de l'éditeur 3Com pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité 3Com 3COM-2006-004 du 19 octobre 2006 :
<http://www.3com.com/securityalert/alerts/3COM-06-004.html>
- Référence CVE CVE-2006-5382 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5382>

Gestion détaillée du document

14 novembre 2006 version initiale.