



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 août 2002
N° CERTA-2002-AVI-181

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des commutateurs Cisco CSS séries 11000

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-181>

Gestion du document

Référence	CERTA-2002-AVI-181
Titre	Vulnérabilité des commutateurs Cisco CSS séries 11000
Date de la première version	19 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

Elévation de privilèges.

2 Systèmes affectés

La série CSS 11000 des commutateurs Cisco CSS (également connus sous le nom Arrowpoint), est composée des modèles CSS 11050, CSS 11150 et CSS 11800. Le logiciel Cisco WebNS permet une gestion de l'équipement grâce à une interface web.

Toutes les versions du logiciel Cisco WebNS sont vulnérables sur l'ensemble des produits de la série CSS 11000. Les autres produits Cisco ne sont pas vulnérables.

3 Résumé

Une vulnérabilité dans la gestion par interface web des commutateurs Cisco CSS séries 1100 permet à un utilisateur mal intentionné d'outrepasser la phase d'authentification.

4 Description

Le logiciel Cisco WebNS permet une gestion des commutateurs CSS grâce à une interface web. Après une phase d'authentification sur le navigateur, l'utilisateur est redirigé vers une URL de gestion de l'équipement.

La connexion directe à cette URL permet à un utilisateur mal intentionné d'accéder à l'interface de gestion sans passer par la phase d'authentification. La connexion directe peut en particulier être facilitée par le stockage de l'adresse dans les favoris du navigateur.

5 Contournement provisoire

- Désactiver la gestion du commutateur via une interface web.
- Filtrer le trafic HTTP vers le commutateur, grâce à une liste de contrôle d'accès. Cette possibilité doit être envisagée avec précaution, car elle peut introduire des effets négatifs. La documentation sur la mise en place de listes de contrôle d'accès sur les équipements CSS se trouve sur le site de Cisco :
<http://www.cisco.com/universcd/cc/td/doc/product/webscale/css/bccfggd/profiles.htm>
<http://www.cisco.com/universcd/cc/td/doc/product/webscale/css/advfcfgd/sqacleql.htm>

6 Solution

La vulnérabilité sera corrigée dans la nouvelle version du logiciel WebNS, qui ne sera pas disponible avant décembre 2002.

7 Documentation

Gestion détaillée du document

19 août 2002 version initiale.