Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 août 2001
N° CERTA-2001-AVI-086

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco CBOS

Gestion du document

Référence	CERTA-2001-AVI-086
Titre	Multiples vulnérabilités dans Cisco CBOS
Date de la première version	27 août 2001
Date de la dernière version	–
Source(s)	Avis Cisco "CBOS web-based configuration utility vulnerability"
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

L'exploitation de ces vulnérabilités permet de réaliser un déni de service.

2 Systèmes affectés

Routeurs Cisco de la famille 600 : 627, 633, 673, 675, 675E, 677, 677i et 678.
Ces modèles sont vulnérables s'ils utilisent une des révisions CBOS suivantes: 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7, 2.3.8, 2.3.9, 2.4.1, 2.4.2, 2.4.2ap.

3 Résumé

CBOS est le "Cisco Broadband Operating System", système d'exploitation utilisé dans les routeurs de la famille 600. Des vulnérabilités dans les utilitaires de configuration accessibles via telnet ou via HTTP permettent à un utilisateur mal intentionné de réaliser un déni de service sur les routeurs.

4 Description

Quand un routeur est accédé par telnet ou HTTP via de multiples connexions, le routeur se met dans un état dans lequel il n'achemine plus aucun trafic et ne répond plus aux tentatives de configuration. Seul un redémarrage de l'équipement permet de le rendre de nouveau opérationnel.

De plus, le service de configuration web (HTTP) est autorisé par défaut et une erreur de CBOS ne permet pas de le désactiver même si dans la configuration le service est désactivé explicitement.

Un utilisateur mal intentionné peut utiliser ces vulnérabilités afin de réaliser à distance un déni de service sur ces routeurs. Il faut souligner que les vers tels que Code Red qui exploitent des vulnérabilités liées à des services accessibles via le port 80 (HTTP) peuvent entrainer aussi un déni de service sur ces équipements (voir CERTA-2001-ALE-008 : Propagation du ver "Code Red").

5 Contournement provisoire

Dans son avis de sécurité (voir "Documentation"), Cisco conseille d'utiliser un port différent du port 80 pour l'utilitaire de configuration Web afin d'empêcher les dénis de service dus aux vers: `set web port xx` où `xx` est un numéro de port >1024.

Une autre solution consiste à désactiver les utilitaires de configuration à distance au moyen de filtres:

```
set filter 0 on deny incoming all 0.0.0.0 0.0.0.0 <ip-routeur> 255.255.255.255
protocol TCP srcport 0-65535 destport 23-23
set filter 1 on deny incoming all 0.0.0.0 0.0.0.0 <ip-routeur> 255.255.255.255
protocol TCP srcport 0-65535 destport 80-80
```

A noter que dans ce cas, seule une console reliée au port série permettra de configurer le routeur. Consultez la documentation Cisco pour plus de renseignements sur l'utilisation des filtres.

6 Solution

Ces vulnérabilités sont corrigées dans les révisions 2.4.2b et 2.4.3 de CBOS.

Contactez votre support Cisco pour l'obtention de ces mises-à-jour.

7 Documentation

Avis Cisco "CBOS web-based configuration utility vulnerability":
http://www.cisco.com/warp/public/707/cisco-cbos-webserver-pub.shtml

Gestion détaillée du document

27 août 2001 version initiale.