



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 décembre 2000
N° CERTA-2000-AVI-083

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les routeurs CISCO serie 600

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-083>

Gestion du document

Référence	CERTA-2000-AVI-083
Titre	Vulnérabilités dans les routeurs CISCO serie 600
Date de la première version	05 décembre 2000
Date de la dernière version	–
Source(s)	FIRST
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

- Déni de service ;
- Contournement des journaux d'enregistrements.

2 Systèmes affectés

Routeurs Cisco CBOS Série 600

3 Résumé

Plusieurs vulnérabilités découvertes dans le système d'exploitation (CBOS) des routeurs CISCO permettent à un utilisateur distant d'engendrer des dénis de service voire de tenter une attaque par force brute sans laisser de traces dans les fichiers journaux.

4 Description

4.1 Première vulnérabilité

Un utilisateur mal intentionné peut, par l'envoi d'une URL malformée sur l'interface web du routeur, provoquer un déni de service.

Nota : Par défaut l'interface Web est désactivée sur les routeurs.

4.2 Deuxième vulnérabilité

Un utilisateur distant peut épuiser toutes les ressources TCP du routeur par l'envoi d'un flux important de connexions TCP SYN.

4.3 Troisième vulnérabilité

Une vulnérabilité présente dans le module d'enregistrement des tentatives de connexions au routeur permet à un utilisateur distant de tenter un accès par force brute (Essais exhaustifs : login - mot de passe) sur l'interface d'administration Web sans que ces tentatives soient enregistrées.

4.4 Quatrième vulnérabilité

Les routeurs CISCO série 600 sont vulnérables à des paquets «ECHO_REQUEST» de grande taille (requête PING), entraînant un arrêt du routeur.

5 Solution provisoire

5.1 Première vulnérabilité

-Restreindre l'accès au serveur Web de gestion :

Dans le mode «enable» :

```
cbos# set web remote [IP MACHINE AUTORISEE]
```

```
cbos# set web remote enabled
```

-Désactiver le serveur Web de gestion :

Dans le mode «enable» :

```
cbos# set web remote disable
```

5.2 Troisième vulnérabilité

-Désactiver le serveur Web de gestion :

Dans le mode «enable» :

```
cbos# set web remote disable
```

5.3 Quatrième vulnérabilité

Filtrer le trafic ICMP ECHO à destination du routeur :

```
cbos# set filter [numéro] on deny incoming all 0.0.0.0
```

```
0.0.0.0 <eth0_IP_address>255.255.255.255 protocol ICMP
```

```
cbos# set filter [numéro+1] on deny incoming all 0.0.0.0
```

```
0.0.0.0 <wan0_IP_address>255.255.255.255 protocol ICMP
```

6 Solution

Correctifs disponible sur le site CISCO :

<http://www.cisco.com>

7 Documentation

Avis CISCO :

<http://www.cisco.com/warp/public/707/CBOS-multiple.shtml>

Gestion détaillée du document

05 décembre 2000 version initiale.