

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité Cisco Cache Engine et Content Engine

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-103>

Gestion du document

Référence	CERTA-2002-AVI-103
Titre	Vulnérabilité Cisco Cache Engine et Content Engine
Date de la première version	16 mai 2002
Date de la dernière version	21 mai 2002
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

- Trafic non sollicité ;
- camouflage d'identité.

2 Systèmes affectés

- Content Engine 507, 560, 590, ou 7320 avec les versions de cache software 2.x, 3.1,4.0.x, ou 4.1.x ;
- Cache Engine 505, 550, ou 570 avec une version de logiciel 2.2.0 ou précédente ;
- Content Router CR-4430 avec ACNS 4.x ;
- Content Distribution Manager CDM-4630 ou CDM-4650 avec ACNS 4.x.

3 Résumé

Un utilisateur mal intentionné peut exploiter une vulnérabilité afin de camoufler son identité et d'effectuer des activités illégales.

4 Description

Les produits Cache Engine et Content Engine de CISCO possèdent des fonctionnalités de cache transparent pour des pages web, ainsi que de serveurs mandataires (proxies) supportant de nombreux protocoles. La configuration par défaut de cette dernière fonctionnalité peut permettre à un individu mal intentionné d'effectuer des connexions réseau non sollicitées et de masquer son identité.

5 Solution

Il est recommandé :

- soit de désactiver la fonction de serveur mandataire HTTPS si celle-ci n'est pas nécessaire :

```
https destination-port deny all
```

- soit de filtrer les requêtes pour les ports autre que HTTPS (443/TCP) :

```
https destination-port allow 443  
https destination-port deny all
```

Se référer au bulletin de sécurité CISCO pour obtenir plus d'informations (cf. Documentation).

6 Documentation

Bulletin de sécurité CISCO "Transparent Cache Engine and Content Engine TCP Relay Vulnerability" :

<http://www.cisco.com/warp/public/707/transparentcache-tcp-relay-vuln-pub.shtml>

Gestion détaillée du document

16 mai 2002 version initiale.

21 mai 2002 correction du lien vers le bulletin CISCO.