

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du Netflow Collection Engine de Cisco

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-2007-AVI-190>

Gestion du document

Référence	CERTA-2007-AVI-190
Titre	Vulnérabilité du Netflow Collection Engine de Cisco
Date de la première version	26 avril 2007
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco 82078 du 25 avril 2007
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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- les versions de Cisco Netflow Collection Engine (NFC) antérieures à 6.0.0.

La version de NFC peut se trouver via le système d'exploitation de la machine hôte, avec la commande :
`/opt/CSCOnfc/nfcollector show-tech`

3 Résumé

Une vulnérabilité a été identifiée dans certaines versions de Cisco Netflow Collection Engine (NFC). Au cours de l'installation, un compte système est créé par défaut, similaire au compte d'accès à l'interface de maintenance. Le mot de passe imposé est identique au nom du compte. Une personne malveillante pourrait donc exploiter cette vulnérabilité pour accéder à l'interface, modifier la configuration, accéder aux données, voire simplement se connecter sur le système hôte avec le compte offert.

4 Description

Une vulnérabilité a été identifiée dans certaines versions de Cisco Netflow Collection Engine (NFC). Netflow est un format particulier permettant d'agréger des paquets réseau (regroupement de paquets suivant certains critères et une fenêtre de temps donnée), qui peut être utilisé pour surveiller le trafic ou détecter certaines anomalies.

Au cours de l'installation, un compte système est créé par défaut, similaire au compte d'accès à l'interface de maintenance. Le mot de passe imposé est identique au nom du compte. Il s'agit de `nfcuser`.

Une personne malveillante pourrait donc exploiter cette vulnérabilité pour accéder à l'interface, modifier la configuration, accéder aux données, voire simplement se connecter sur le système hôte avec le compte offert.

L'avis de sécurité Cisco indique les commandes pour changer cette configuration, ainsi que les mises à jour. Celles-ci sont cependant facultatives dans le cas présent.

5 Solution

Se référer à l'avis de sécurité de l'éditeur Cisco pour de plus amples détails (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco ID 82078 du 25 avril 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070425-nfc.shtml>

Gestion détaillée du document

26 avril 2007 version initiale.