Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 janvier 2008
N° CERTA-2008-AVI-037

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans des produits Cisco

Gestion du document

Référence	CERTA-2008-AVI-037
Titre	Vulnérabilités dans des produits Cisco
Date de la première version	24 janvier 2008
Date de la dernière version	–
Source(s)	Avis de sécurité de Cisco publiés le 23 janvier 2008
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Les solutions Cisco PIX et ASA ayant des versions logicielles antérieures à 7.2(3)006 ou 8.0(3) ;
- Les solutions Cisco Application Velocity System (AVS) 3110, 3120, 3180 et 3180A Management Station ayant des versions logicielles antérieures à AVS 5.1.0.

3 Résumé

Deux vulnérabilités ont été identifiées dans des produits Cisco. La première concerne l'absence de changement de mot de passe des utilisateurs pendant la phase initiale de configuration pour les solutions Cisco AVS. La seconde concerne le traitement du champ `Time-To-Live` des trames IP par des solutions PIX et ASA.

4 Description

Deux vulnérabilités ont été identifiées dans des produits Cisco :

1. La première concerne l'absence de changement de mot de passe de certains utilisateurs pendant la phase initiale de configuration pour les solutions Cisco AVS. Ces utilisateurs par défaut peuvent avoir des droits d'administrateur. Si l'administrateur ne change pas ces identifiants de lui-même, ces comptes restent actifs et présents sur le système, permettant ainsi à une personne malveillante d'élever ses privilèges et de modifier les configurations.
2. La seconde concerne le traitement du champ `Time-To-Live` des trames IP par des solutions PIX et ASA. Certaines valeurs provoqueraient le redémarrage du système. Cette vulnérabilité fonctionne dès lors que l'option `decrement-ttl` est fonctionnelle. Celle-ci n'est cependant pas active par défaut.

5 Solution

Se référer aux bulletins de sécurité de Cisco pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco 20080123-asa du 23 janvier 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml
- Bulletin de sécurité Cisco 20080123-avs du 23 janvier 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.shtml
- Référence CVE CVE-2008-0028 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0028
- Référence CVE CVE-2008-0029 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0029

Gestion détaillée du document

24 janvier 2008 version initiale.