

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco Firewall Services Module

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-2011-AVI-565>

Gestion du document

Référence	CERTA-2011-AVI-565
Titre	Multiples vulnérabilités dans Cisco Firewall Services Module
Date de la première version	13 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20111005-fwsm du 13 octobre 2011
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 ;
- déni de service à distance.

2 Systèmes affectés

- Switch Cisco série Catalyst 6500;
- routeurs Cisco série 7600.

3 Résumé

Plusieurs vulnérabilités permettant à un attaquant distant, soit de forcer l'équipement Cisco vulnérable à redémarrer, soit de contourner des politiques de sécurité ont été corrigées.

4 Description

Une première vulnérabilité affecte le système de journalisation *syslog* (CVE-2011-3296), dans le cas où l'équipement est configuré de la manière suivante :

- l'appareil possède des interfaces avec des adresses IPv6 ;

- la journalisation est activée (commande « logging enable »);
- le niveau de journalisation est de 6 ou 7, ou des messages de type 302015 sont créés manuellement.

Les équipements configurés pour utiliser le mode AAA (*Authentication, Authorization and Accounting*) sont vulnérables à une attaque en déni de service (CVE-2011-3297).

Une vulnérabilité dans l'implémentation du protocole TACACS+ (*Terminal Access Controller Access-Control System Plus*) permet à un attaquant distant de contourner les règles de contrôle d'accès gérées par ce protocole (CVE-2011-3298).

Quatre vulnérabilités dans le système d'inspection des paquets du protocole SunRPC permettent à une personne malintentionnée de provoquer l'arrêt de l'appareil à distance au moyen de messages spécialement construits (CVE-2011-3299, CVE-2011-3300, CVE-2011-3301 et CVE-2011-3302).

Enfin, une vulnérabilité dans le système d'inspection de paquets du protocole ILS permet à un attaquant de réaliser un déni de service lorsque celui-ci dirige du trafic spécialement conçu au travers de l'équipement vulnérable. L'équipement doit avoir activé l'inspection des paquets ILS (CVE-2011-3303).

5 Contournement provisoire

Différents contournements sont proposés par l'éditeur en fonction des vulnérabilités :

- désactiver la journalisation des messages de type 302015 (commande `no logging message 302015`) bloque la vulnérabilité CVE-2011-3297 ;
- désactiver l'inspection des paquets SunRPC (commande `no inspect sunrpc`) bloque les vulnérabilités CVE-2011-3299, CVE-2011-3300, CVE-2011-3301 et CVE-2011-3302 ;
- désactiver l'inspection des paquets ILS (commande `no inspect ils`) bloque la vulnérabilité CVE-2011-3303.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Cisco 20111005-fwsm du 13 octobre 2011 :
<http://www.cisco.com/warp/public/707/cisco-sa-20111005-fwsm.shtml>
- Référence CVE CVE-2011-3296 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3296>
- Référence CVE CVE-2011-3297 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3297>
- Référence CVE CVE-2011-3298 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3298>
- Référence CVE CVE-2011-3299 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3299>
- Référence CVE CVE-2011-3300 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3300>
- Référence CVE CVE-2011-3301 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3301>
- Référence CVE CVE-2011-3302 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3302>
- Référence CVE CVE-2011-3303 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3303>

Gestion détaillée du document

13 octobre 2011 version initiale.