Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 septembre 2011
N° CERTA-2011-AVI-544

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la fonction NAT de CISCO IOS

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-544

Gestion du document

Référence	CERTA-2011-AVI-544
Titre	Multiples vulnérabilités dans la fonction NAT de CISCO IOS
Date de la première version	30 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20110928-nat du 28 septembre 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

Déni de service à distance.

2 Systèmes affectés

- CISCO IOS versions 12.1, 12.2, 12.3, 12.4, 15.0 et 15.1 ;
- CISCO IOS XE.

Se référer au bulletin de sécurité de l'éditeur pour le détail des versions affectées.

3 Résumé

De multiples vulnérabilités dans la fonction NAT de CISCO IOS peuvent provoquer des dénis de service à distance.

4 Description

De multiples vulnérabilités ont été corrigées dans CISCO IOS. Ces vulnérabilités concernent la fonction de traduction d'adresse réseau (NAT) pour les protocoles LDAP, SIP et H323. L'exploitation de ces vulnérabilités, par l'envoi de paquets réseaux spécialement conçus, peut provoquer le redémarrage de l'équipement ou son blocage.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 20110928-nat du 28 septembre 2011 :
  http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml
- Référence CVE CVE-2011-0946 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0946
- Référence CVE CVE-2011-3276 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3276
- Référence CVE CVE-2011-3277 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3277
- Référence CVE CVE-2011-3279 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3279
- Référence CVE CVE-2011-3280 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3280

Gestion détaillée du document

30 septembre 2011 version initiale.