Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 septembre 2013
N° CERTA-2013-AVI-544

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco IOS

Gestion du document

Référence	CERTA-2013-AVI-544
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	26 septembre 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20130925-dhcp du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-rsvp du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-ike du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-ipv6vfr du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-nat du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-wedge du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-cce du 25 septembre 2013 Bulletin de sécurité Cisco cisco-sa-20130925-ntp du 25 septembre 2013
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(s)

- déni de service à distance
- déni de service

2 - Systèmes affectés

- Cisco IOS
- Cisco IOS XE

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Cisco IOS*. Elles permettent à un attaquant de provoquer un déni de service à distance et un déni de service.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Cisco cisco-sa-20130925-dhcp du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp
- Bulletin de sécurité Cisco cisco-sa-20130925-rsvp du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-rsvp
- Bulletin de sécurité Cisco cisco-sa-20130925-ike du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ike
- Bulletin de sécurité Cisco cisco-sa-20130925-ipv6vfr du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ipv6vfr
- Bulletin de sécurité Cisco cisco-sa-20130925-nat du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-nat
- Bulletin de sécurité Cisco cisco-sa-20130925-wedge du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-wedge
- Bulletin de sécurité Cisco cisco-sa-20130925-cce du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-cce
- Bulletin de sécurité Cisco cisco-sa-20130925-ntp du 25 septembre 2013
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ntp
- Référence CVE CVE-2013-5472
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5472
- Référence CVE CVE-2013-5473
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5473
- Référence CVE CVE-2013-5474
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5474
- Référence CVE CVE-2013-5475
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5475
- Référence CVE CVE-2013-5476
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5476
- Référence CVE CVE-2013-5477
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5477
- Référence CVE CVE-2013-5478
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5478
- Référence CVE CVE-2013-5479
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5479
- Référence CVE CVE-2013-5480
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5480
- Référence CVE CVE-2013-5481
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5481

Gestion détaillée du document

26 septembre 2013 version initiale.