

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2013-AVI-205>

Gestion du document

Référence	CERTA-2013-AVI-205
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	28 mars 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco du 27 mars 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

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.

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-20130327-rsvp du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp>
- Bulletin de sécurité cisco cisco-sa-20130327-cce du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-cce>
- Bulletin de sécurité cisco cisco-sa-20130327-pt du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-pt>
- Bulletin de sécurité cisco cisco-sa-20130327-ike du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ike>
- Bulletin de sécurité cisco cisco-sa-20130327-smartinstall du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall>
- Bulletin de sécurité cisco cisco-sa-20130327-nat du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat>
- Bulletin de sécurité cisco cisco-sa-20130327-ipsla du 27 mars 2013
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ipsla>
- Référence CVE CVE-2013-1142
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1142>
- Référence CVE CVE-2013-1143
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1143>
- Référence CVE CVE-2013-1144
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1144>
- Référence CVE CVE-2013-1145
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1145>
- Référence CVE CVE-2013-1146
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1146>
- Référence CVE CVE-2013-1147
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1147>
- Référence CVE CVE-2013-1148
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1148>

Gestion détaillée du document

28 mars 2013 version initiale.