

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les commutateurs Cisco Catalyst et les routeurs Cisco Integrated Services

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-540>

Gestion du document

Référence	CERTA-2011-AVI-540
Titre	Vulnérabilité dans les commutateurs Cisco Catalyst et les routeurs Cisco Integrated Services
Date de la première version	29 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20110928-smart-install 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Les commutateurs Cisco Catalyst ;
- les routeurs Cisco Integrated Services.

3 Résumé

Une vulnérabilité dans les commutateurs Cisco Catalyst et les routeurs Cisco Integrated Services permet à une personne distante malintentionnée d'exécuter du code arbitraire.

4 Description

Une vulnérabilité dans la fonctionnalité *Smart Install* des commutateurs Cisco Catalyst et des routeurs Cisco Integrated Services permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

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-smart-install du 28 septembre 2011 :
<http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.shtml>
- Référence CVE CVE-2011-3271 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3271>

Gestion détaillée du document

29 septembre 2011 version initiale.