

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco IronPort

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-2012-AVI-090>

Gestion du document

Référence	CERTA-2012-AVI-090
Titre	Vulnérabilité dans Cisco IronPort
Date de la première version	20 février 2012
Date de la dernière version	–
Source	Bulletin de sécurité Cisco IntelliShield 25045 du 13 février 2012
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

Injection de code indirecte à distance.

2 Systèmes affectés

Cisco IronPort Encryption Appliance.

3 Résumé

Une vulnérabilité dans Cisco IronPort Encryption Appliance permet à un attaquant de réaliser de l'injection de code indirecte à distance.

4 Description

Une vulnérabilité de l'interface d'administration de Cisco IronPort Encryption Appliance permet à un attaquant distant non authentifié de réaliser de l'injection de code indirecte (XSS).

5 Solution

La version 6.5.3 du logiciel de Cisco IronPort Encryption Appliance corrige ce problème.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco IntelliShield 25045 du 13 février 2012 :
<http://tools.cisco.com/security/center/viewAlert.x?alertId=25045>
- Référence CVE CVE-2012-0340 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0340>

Gestion détaillée du document

20 février 2012 version initiale.