

Affaire suivie par :
CERTA

BULLETIN D'ALERTE 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-ALE-001>

Gestion du document

Référence	CERTA-2012-ALE-001-001
Titre	Vulnérabilité dans Cisco IronPort
Date de la première version	01 février 2012
Date de la dernière version	05 février 2013
Source	Bulletin de sécurité Cisco 20120126-ironport du 26 janvier 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Cisco IronPort Email Security Appliance, C-series et M-Series, versions antérieures à la version 7.6.0 ;
- Cisco IronPort Security Management Appliance, M-Series, versions antérieures à la version 7.8.0.

3 Résumé

Une vulnérabilité sur certains boîtiers Cisco IronPort permet à un attaquant d'exécuter du code arbitraire à distance.

4 Description

Certains boîtiers Cisco IronPort utilisent une version vulnérable du démon *telnetd*. Ce démon est actif par défaut sur l'interface d'administration. Cette vulnérabilité permet à un attaquant 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 20120126-ironport du 26 janvier 2012 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport>
- Référence CVE CVE-2011-4862 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4862>

Gestion détaillée du document

01 février 2012 version initiale ;

05 février 2013 fermeture de l'alerte, suite à la correction par l'éditeur.