

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Cisco Network Building Mediator

---

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-2010-AVI-229>

---

### Gestion du document

Référence	CERTA-2010-AVI-229
Titre	Multiples vulnérabilités dans Cisco Network Building Mediator
Date de la première version	27 mai 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20100526-mediator du 26 mai 2010
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

- Accès au système ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- Produits *Richards-Zeta Mediator 2500* ;
- *Cisco Network Building Mediator* modèles NBM-2400 et NBM-4800.

Toutes les versions du logiciel *Mediator Framework* antérieures à 3.1.1 sont affectées.

## 3 Résumé

De multiples vulnérabilités dans *Cisco Network Building Mediator* permettent notamment d'obtenir un accès administrateur au système.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Cisco Network Building Mediator* :

- des identifiants par défaut sont assignés à de nombreux comptes, incluant celui de l'administrateur (CVE-2010-0595) ;
- des utilisateurs authentifiés, ne disposant pas des droits requis, peuvent lire et modifier la configuration du matériel (CVE-2010-0596 et CVE-2010-0597) ;
- les identifiants de connexion peuvent être interceptés (CVE-2010-0598 et CVE-2010-0599) ;
- un attaquant peut lire les fichiers de configuration du système et obtenir notamment la liste des comptes et leur mot de passe associé. Cette attaque ne nécessite pas d'authentification préalable (CVE-2010-0600).

## 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 20100526-mediator du 26 mai 2010 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20100526-mediator.shtml>
- Référence CVE CVE-2010-0595 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0595>
- Référence CVE CVE-2010-0596 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0596>
- Référence CVE CVE-2010-0597 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0597>
- Référence CVE CVE-2010-0598 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0598>
- Référence CVE CVE-2010-0599 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0599>
- Référence CVE CVE-2010-0600 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0600>

## Gestion détaillée du document

27 mai 2010 version initiale.