



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 15 novembre 2011
N° CERTA-2011-AVI-638

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans des produits Cisco TelePresence et Tandberg

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-638>

Gestion du document

Référence	CERTA-2011-AVI-638
Titre	Vulnérabilités dans des produits Cisco TelePresence et Tandberg
Date de la première version	15 novembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20111109-telepresence-c-ex-series Bulletin de sécurité Cisco cisco-sa-20110202-tandberg
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco TelePresence System Integrator C Series avec les versions logicielles TC4.0, TC4.1 ou TC4.2 ;
- Cisco TelePresence Ex C Series avec les versions logicielles TC4.0, TC4.1 ou TC4.2 ;
- Cisco TelePresence Quick Set avec les versions logicielles TC4.0, TC4.1 ou TC4.2 ;
- Tandberg E, EX et C Series Endpoints avec les versions logicielles antérieures à TC4.0.

3 Résumé

Un défaut de configuration dans les produits cités plus haut pourrait permettre à une personne malveillante de prendre le contrôle total du système à distance.

4 Description

Les dispositifs *Tandberg* possèdent leur compte administrateur (*root*) activé par défaut, sans mot de passe, ce qui était initialement prévu pour des tâches de débogage mais non nécessaire lors des opérations normales.

Certains dispositifs *Cisco TelePresence* ont été distribués avec une configuration non sécurisée. La vulnérabilité est due à un échec de restauration de la configuration par défaut après avoir fait des tests et configuré des options. Ces dispositifs pourraient avoir leur compte administrateur (*root*) activé et configuré avec un mot de passe connu.

Une personne malveillante pourrait prendre le contrôle total d'un de ces systèmes à distance.

5 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco 20111109-telepresence-c-ex-series du 09 novembre 2011 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111109-telepresence-c-ex-series>
- Bulletin de sécurité Cisco 20110202 du 2 février 2011 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110202-tandberg>
- Référence CVE CVE-2011-0354 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0354>

Gestion détaillée du document

15 novembre 2011 version initiale.