

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco IP Video Phone E20

---

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-035>

---

### Gestion du document

Référence	CERTA-2012-AVI-035
Titre	Vulnérabilité dans Cisco IP Video Phone E20
Date de la première version	31 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20120118-te du 18 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

Accès d'administration à distance.

## 2 Systèmes affectés

*Cisco TelePresence Software* version TE 4.1.0.

## 3 Résumé

Une vulnérabilité dans *Cisco IP Video Phone E20* permet d'obtenir un accès d'administration à distance.

## 4 Description

Un compte d'administration (*root*) a été découvert dans *Cisco TelePresence Software* en version TE 4.1.0, inclus dans le matériel *Cisco IP Video Phone E20*. En théorie, ce compte devrait être désactivé, mais si le matériel a utilisé une version antérieure de *Cisco TelePresence Software* avant le déploiement d'une mise-à-jour, alors il est possible qu'une erreur ait maintenu le compte *root* actif. Ce dernier est accessible via SSH avec un mot de passe par défaut.

## **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 20120118-te du 18 janvier 2012 :  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120118-te>
- Référence CVE CVE-2011-4659 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4659>

## **Gestion détaillée du document**

**31 janvier 2012** version initiale.