

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les postes téléphoniques Cisco Unified Phones 7900 Series

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-328>

Gestion du document

Référence	CERTA-2011-AVI-328
Titre	Vulnérabilités dans les postes téléphoniques Cisco Unified Phones 7900 Series
Date de la première version	03 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20110601-phone du 01 juin 2011
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco Unified IP Phone 7975G ;
- Cisco Unified IP Phone 7971G-GE ;
- Cisco Unified IP Phone 7970G ;
- Cisco Unified IP Phone 7965G ;
- Cisco Unified IP Phone 7962G ;
- Cisco Unified IP Phone 7961G ;
- Cisco Unified IP Phone 7961G-GE ;
- Cisco Unified IP Phone 7945G ;
- Cisco Unified IP Phone 7942G ;
- Cisco Unified IP Phone 7941G ;
- Cisco Unified IP Phone 7941G-GE ;
- Cisco Unified IP Phone 7931G ;

- Cisco Unified IP Phone 7911G ;
- Cisco Unified IP Phone 7906G ;

3 Résumé

Plusieurs vulnérabilités permettant une élévation de privilège ainsi qu'un contournement de la politique de sécurité ont été découvertes dans différents produits de la gamme *Cisco Unified IP Phones 7900 Series*.

4 Description

Trois failles ont été découvertes dans plusieurs produits de la gamme *Cisco Unified IP Phones 7900 Series*.

Deux de ces failles (CVE-2011-1602 et CVE-2011-1603) permettent à une personne malintentionnée d'élever ses privilèges et, ainsi, de modifier la configuration du poste, voir d'obtenir des informations sensibles.

La troisième faille (CVE-2011-1637) permet à un utilisateur malintentionné de contourner la vérification des signatures de l'image logicielle chargée sur le téléphone.

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 20110601-phone du 01 juin 2011 :
<http://www.cisco.com/warp/public/707/cisco-sa-20110601-phone.shtml>
- Référence CVE CVE-2011-1602 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1602>
- Référence CVE CVE-2011-1603 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1603>
- Référence CVE CVE-2011-1637 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1637>

Gestion détaillée du document

03 juin 2011 version initiale.