

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco Unified Communications Manager

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-2008-AVI-255>

Gestion du document

Référence	CERTA-2008-AVI-255
Titre	Multiples vulnérabilités dans Cisco Unified Communications Manager
Date de la première version	20 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco n°100995 du 14 mai 2008
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

Déni de service à distance.

2 Systèmes affectés

- Cisco Unified Communications Manager 4.x ;
- Cisco Unified Communications Manager 5.x ;
- Cisco Unified Communications Manager 6.x.

3 Résumé

De multiples vulnérabilités sont présentes dans Cisco Unified Communications Manager permettant à un utilisateur distant de provoquer un déni de service de l'équipement vulnérable.

4 Description

Plusieurs vulnérabilités sont présentes dans Cisco Unified Communications Manager :
– la première, relative au Certificate Trust List Provider (CTL Provider) de la version 5.x

de CUCM, permet à un utilisateur distant de provoquer un déni de service via une série de paquets envoyés sur le port 2444/TCP de l'équipement ;

- une seconde, relative au même composant (CTL Provider) mais des versions 5.x et 6.x des CUCM, permet à un utilisateur distant de provoquer une consommation excessive de mémoire sur l'équipement vulnérable via une série de paquets sur le port 2444/TCP ;
- une troisième est présente dans la Certificate Authority Proxy Function (CAFP) et peut être exploitée par le biais d'un envoi d'un paquet particulier sur le port 3804/TCP pour causer un déni de service d'un CUCM versions 4.1, 4.2 ou 4.3 ;
- une quatrième vulnérabilité permet de causer un déni de service des CUCM versions 5.x et 6.x via l'envoi de messages SIP de type JOIN construits de façon particulière ;
- une cinquième peut être exploitée via un envoi de paquets SIP de type INVITE pour provoquer un déni de service sur les CUCM versions 4.1, 4.2, 4.3, 5.x et 6.x ;
- la dernière vulnérabilité concerne le service SNMP Trap Agent et permet à un utilisateur distant de provoquer un déni de service sur les versions 4.1, 4.2, 4.3, 5.x et 6.x des CUCM via des paquets UDP sur le port 61441/TCP de l'équipement vulnérable.

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 ID 100995 du 14 mai 2008 :
<http://www.cisco.com/warp/public/707/cisco-sa-20080514-cucmdos.shtml>
- Référence CVE CVE-2008-1742 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1742>
- Référence CVE CVE-2008-1743 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1743>
- Référence CVE CVE-2008-1744 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1744>
- Référence CVE CVE-2008-1745 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1745>
- Référence CVE CVE-2008-1746 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1746>
- Référence CVE CVE-2008-1747 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1747>
- Référence CVE CVE-2008-1748 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1748>

Gestion détaillée du document

20 mai 2008 version initiale.