

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Collaboration Server

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-2004-AVI-218>

Gestion du document

Référence	CERTA-2004-AVI-218
Titre	Vulnérabilité dans Cisco Collaboration Server
Date de la première version	02 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité SA-20040630 de CISCO
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

- Atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco Collaboration Server 4.x avec ServletExec 3.0 ;
- Cisco Collaboration Server 3.x avec ServletExec 2.2 ;
- Cisco Collaboration Server 5.x avec ServletExec 4.1.

3 Résumé

Une vulnérabilité a été découverte dans Cisco Collaboration Server installé avec ServletExec permettant à un individu mal intentionné d'installer des fichiers sur le système vulnérable et d'élever ses privilèges.

4 Description

Cisco Collaboration Server (CCS) est une solution de travail collaboratif pouvant être intégrée à des architectures de commerce électronique ou de service client.

CCS utilise la servlet Java ServletExec maintenue par la société New Atlanta.

Une vulnérabilité présente dans ServletExec permet de télécharger des fichiers sur le serveur Web et de les exécuter afin d'élever ses privilèges.

5 Solution

- Appliquer les correctifs à l'aide du script fourni par Cisco pour CSS 4.x :
<http://www.cisco.com/cgi-bin/tablebuild.pl/ccs40>
- mettre à jour CCS avec la version 5.x (cf. Documentation) ;
- correctifs pour ServletExec de New Atlanta :
<ftp://ftp.newatlanta.com/public/servletexec/>

6 Documentation

Bulletin de sécurité SA-20040630 de CISCO :

<http://www.cisco.com/warp/public/707/cisco-sa-20040630-CCS.shtml>

Gestion détaillée du document

02 juillet 2004 version initiale.