

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CiscoWorks Common Services

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-2010-AVI-517>

Gestion du document

Référence	CERTA-2010-AVI-517
Titre	Vulnérabilités dans CiscoWorks Common Services
Date de la première version	28 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20101027-cs du 27 octobre 2010
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- CiscoWorks Common Services versions 3.0.5 et postérieures pour Microsoft Windows et Oracle Solaris. Les versions 4.0 et postérieures corrigent cette vulnérabilité ;
- CiscoWorks Common Services est inclus dans de nombreux produits Cisco. La liste complète des logiciels Cisco contenant une version vulnérable du logiciel est disponible dans l'avis publié sur le site de l'éditeur.

3 Résumé

CiscoWorks Common Services est une application résidante dans les outils d'administration de réseau édités par Cisco. Une vulnérabilité a été corrigée qui permet l'exécution de code arbitraire à distance.

4 Description

CiscoWorks Common Services est un ensemble de modules sous-jacents qui fournit des services communs aux outils d'administration de réseau édités par Cisco. Une vulnérabilité de type débordement de mémoire a été

corrigée dans le module serveur Web. L'exploitation de cette vulnérabilité permet à un attaquant d'exécuter du code arbitraire à distance avec les privilèges d'un administrateur.

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 20101027-cs du 27 octobre 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20101027-cs.shtml>
- Référence CVE CVE-2010-3036 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3036>

Gestion détaillée du document

28 octobre 2010 version initiale.