

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans CiscoWorks

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-2007-AVI-530>

Gestion du document

Référence	CERTA-2007-AVI-530
Titre	Vulnérabilité dans CiscoWorks
Date de la première version	07 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Cisco 100240 du 5 décembre 2007
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

Injection de code indirecte.

2 Systèmes affectés

- CiscoWorks Common Services 3.0.x;
- CiscoWorks Common Services 3.1.

3 Résumé

L'interface `CiscoWorks` contient une vulnérabilité permettant de réaliser une injection de code indirecte.

4 Description

`CiscoWorks` est une suite d'outils, réalisés en Java, utilisés pour paramétrer les réseaux possédant des équipements `Cisco`. Ils sont accessibles via une interface web qui accepte des arguments qui ne sont pas correctement contrôlés. Un utilisateur malveillant peut utiliser ces arguments pour réaliser une injection de code indirecte et exécuter du code web arbitraire (HTTP et script) dans le navigateur d'un utilisateur et cela dans le contexte du site `CiscoWorks`.

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 100240 du 05 décembre 2007 :
<http://www.cisco.com/warp/public/707/cisco-sr-20071205-cws.shtml>
- Référence CVE CVE-2007-5582 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5582>

Gestion détaillée du document

07 décembre 2007 version initiale.