Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 06 juin 2011
N° CERTA-2011-AVI-329

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco AnyConnect Secure Mobility Client

Gestion du document

Référence	CERTA-2011-AVI-329
Titre	Vulnérabilités dans Cisco AnyConnect Secure Mobility Client
Date de la première version	06 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20110601-ac 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

- Exécution de code arbitraire à distance ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco AnyConnect Secure Mobility Client pour Microft Windows, versions antérieures à 2.3.254 ;
- Cisco AnyConnect Secure Mobility Client pour Linux et MacOS X, toutes versions majeures autres que 2.5.x et 3.0.x ainsi que les versions 2.5.x antérieures à 2.5.3041 et 3.0.x antérieures à 3.0.629.

3 Résumé

Plusieurs vulnérabilités permettant une exécution de code à distance ainsi qu'une élévation de privilèges ont été découvertes dans *Cisco AnyConnect Secure Mobility Client*.

4 Description

Deux vulnérabilités sont présentes dans *Cisco AnyConnect Secure Mobility Client*.

La première (CVE-2011-2041) permet à un utilisateur malintentionné d'élever ses privilèges. Cette vulnérabilité ne touche que les versions de *Cisco AnyConnect Secure Mobility Client* destinées à *Windows*.

La seconde (CVE-2011-2039 et CVE-2011-2040) permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance. Cette faille provient d'un manque de vérification du programme téléchargé lors du déploiement distant de *Cisco AnyConnect Secure Mobility Client*. Un attaquant pourrait ainsi contrefaire la page de déploiement de l'application et amener un utilisateur à télécharger un programme malveillant qui sera exécuté par l'assistant de déploiement. Les versions de *Cisco AnyConnect Secure Mobility Client* pour *Windows* supérieures à 2.3.185 ne sont pas affectées par cette vulnérabilité.

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-ac du 01 juin 2011 :
  http://www.cisco.com/warp/public/707/cisco-sa-20110601-ac.shtml
- Référence CVE CVE-2011-2039 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2039
- Référence CVE CVE-2011-2040 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2040
- Référence CVE CVE-2011-2041 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2041

Gestion détaillée du document

06 juin 2011 version initiale.