



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 mai 2007
N° CERTA-2007-AVI-224

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans des produits Cisco

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-224>

Gestion du document

Référence	CERTA-2007-AVI-224
Titre	Multiples vulnérabilités dans des produits Cisco
Date de la première version	24 mai 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Cisco du 22 et 23 mai 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Cisco IOS 12.4 ainsi que les versions antérieures ;
- Cisco IOS XR ;
- Cisco PIX et ASA Security Appliances ;
- Cisco Firewall Service Module (FWSM) ;
- Cisco Unified CallManager CCM 4.1, ainsi que les versions antérieures.

3 Description

Plusieurs vulnérabilités ont été rendues publiques cette semaine, concernant des produits Cisco. Parmi eux :

- les systèmes fonctionnant avec le système d'exploitation IOS ne manipuleraient pas correctement certains paquets SSL (pour *Secure Sockets Layer*). Plus précisément, les vulnérabilités surviennent au moment des négociations, avec les messages `ClientHello`, `ChangeCipherSpec` et `FinishedMessages`. Les

détails protocolaires sont décrits dans le RFC 4346. Une personne malveillante peut exploiter l'une de ces vulnérabilités après avoir établi une connexion TCP valide, ou en injectant des paquets entre deux machines victimes. Le système ayant une version IOS vulnérable pourrait alors être perturbé.

- une bibliothèque cryptographique tierce utilisée par plusieurs produits Cisco ne manipulerait pas correctement certaines données codées en ASN.1 (*Abstract Syntax Notation One*). L'exploitation de cette vulnérabilité entraîne la perturbation du système, et ne nécessite pas l'utilisation de certificats ou autres crédits (identifiants et mots de passe) valides.
- une vulnérabilité de type « injection de code indirecte » (ou *Cross-Site Scripting*) existerait dans l'interface Web de Cisco CallManager. Les données entrées par le formulaire de recherche ne sont pas correctement contrôlées. Une personne malveillante pourrait inciter un utilisateur à cliquer sur un lien réticulaire particulier exploitant cette vulnérabilité, afin de provoquer l'exécution de scripts via son navigateur.

4 Solution

Se référer aux différents bulletins de sécurité de l'éditeur Cisco pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Cisco ID 91890 du 22 mai 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>
- Bulletin de sécurité Cisco ID 91888 du 22 mai 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>
- Bulletin de sécurité Cisco ID 82462 du 23 mai 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070523-ccm.shtml>
- Référence CVE CVE-2006-3894 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3894>
- Référence CVE CVE-2007-2813 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2813>
- Référence CVE CVE-2007-2832 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2832>

Gestion détaillée du document

24 mai 2007 version initiale.