Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 octobre 2007
N° CERTA-2007-AVI-449

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité EAP dans les produits Cisco

Gestion du document

Référence	CERTA-2007-AVI-449
Titre	Vulnérabilité EAP dans les produits Cisco
Date de la première version	22 octobre 2007
Date de la dernière version	–
Source(s)	Réponse de sécurité Cisco 98727 du 19 octobre 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

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

L'ensemble des éléments Cisco mettant en œuvre le protocole EAP seraient vulnérables. Cela comprend en particulier les points d'accès sans-fil et les commutateurs fonctionnant sous Cisco IOS ou Cisco CatOS.

Une liste complète des éléments vulnérables est disponible aux clients Cisco sous les identifiants de bogues CSCsj56438, CSCsb45696 et CSCsc55249.

3 Résumé

Une vulnérabilité a été identifiée dans la mise en œuvre du protocole EAP des produits Cisco. L'exploitation de cette dernière par le biais de paquets spécialement construits permettrait de perturber le fonctionnement du sytème.

4 Description

EAP (pour *Extensible Authentication Protocol*) est un mécanisme d'authentification défini dans le RFC 3748. Il peut être mis en place dans des architectures aussi bien filaires que sans-fil, et prendre différentes formes, dont LEAP (*Lightweight Extensible Authentication Protocol*) développé par Cisco Systems, ou EAP-TLS, EAP-TTLS, PEAP, etc.

Une vulnérabilité a été identifiée dans la mise en œuvre du protocole EAP des produits Cisco. Ils ne manipuleraient pas correctement des paquets de réponse EAP, ce qui pourrait être exploité par une personne malveillante à distance afin de perturber le fonctionnement du système. La réception d'un paquet construit à de mauvaises fins est facilitée dans le cas d'une architecture sans-fil.

5 Solution

Se référer au bulletin de sécurité de l'éditeur Cisco pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco ID 98727 du 19 octobre 2007 :
  http://www.cisco.com/warp/public/707/cisco-sr-20071019-eap.shtml
- RFC 3748, "Extensible Authentication Protocol (EAP)", juin 2004 :
  http://www.ietf.org/rfc/rfc3748.txt

Gestion détaillée du document

22 octobre 2007 version initiale.