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 décembre 2005
N° CERTA-2005-AVI-458-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la solution IPsec Openswan

Gestion du document

Référence	CERTA-2005-AVI-458-002
Titre	Vulnérabilité de la solution IPsec Openswan
Date de la première version	16 novembre 2005
Date de la dernière version	22 décembre 2005
Source(s)	Avis de sécurité 273756/NISCC/ISAKMP de l'UNIRAS
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 distant.

2 Systèmes affectés

Tout système Linux utilisant `Openswan` dans une version 2 antérieure à la 2.4.4.

3 Résumé

Un utilisateur mal intentionné peut envoyer des paquets volontairement mal formés au service IKE pour provoquer son arrêt et empêcher ainsi l'établissement de toute nouvelle connexion.

4 Description

`Openswan` est une solution IPsec pour système d'exploitation `Linux`.
Une faille dans le gestionnaire IKE des associations de sécurité peut être exploitée pour provoquer un déni de service. Par ailleurs, un problème lié à la négociation du chiffrement 3DES est également corrigé.

5 Solution

Mettre à jour les sources en version 2.4.4 au moins, ou se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site internet d'`Openswan` :
  http://www.openswan.org
- Avis de sécurité `Openswan` du 14 novembre 2005 :
  http://www.openswan.org/niscc2/
- Mise à jour de sécurité Fedora Core 3 FEDORA-2005-1092 du 21 novembre 2005 :
  http://www.redhat.com/archives/fedora-announce-list/2005-November/msg00057.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-1093 du 21 novembre 2005 :
  http://www.redhat.com/archives/fedora-announce-list/2005-November/msg00058.html
- Bulletin de sécurité Gentoo GLSA 200512-04 du 12 décembre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200512-04.xml
- Bulletin de sécurité SUSE SuSE-SA:2005:070 du 20 décembre 2005 :
  http://www.novell.com/linux/security/advisories/2005_70_ipsec.html
- Référence CVE CVE-2005-3671 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3671
- Avis de sécurité de l'UNIRAS 273756/NISCC/ISAKMP du 14 novembre 2005 :
  http://www.uniras.gov.uk/niscc/docs/br-20051114-01013.html
- Note de vulnérabilité #226364 de l'US-CERT :
  http://www.kb.cert.org/vuls/id/226364

Gestion détaillée du document

16 novembre 2005 version initiale ;

20 décembre 2005 ajout des bulletins de sécurité Gentoo, Fedora Core 3 et 4, de la référence CVE, de la note de vulnérabilité US-CERT et correction du numéro de version des sources vulnérables ;

22 décembre 2005 ajout du bulletin de sécurité SuSE.