



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 mars 2005
N° CERTA-2005-AVI-117-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans OpenSLP

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-2005-AVI-117>

Gestion du document

Référence	CERTA-2005-AVI-117-002
Titre	Vulnérabilités dans OpenSLP
Date de la première version	15 mars 2005
Date de la dernière version	24 mars 2005
Source(s)	Bulletin de sécurité SUSE
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

- Execution de code arbitraire ;
- déni de service.

2 Systèmes affectés

OpenSLP versions 1.x antérieures à la version 1.2.1.

3 Résumé

Plusieurs vulnérabilités présentes dans OpenSLP peuvent être exploitées par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire à distance sur un système vulnérable.

4 Description

Plusieurs débordements de mémoire ont été découverts dans OpenSLP. Un utilisateur mal intentionné peut, via des paquets SLP (Service Location Protocol) malicieusement construits, réaliser un déni de service ou exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Site de SUSE :
<http://www.suse.com>
- Mise à jour en version 1.2.1 :
http://sourceforge.net/project/showfiles.php?group_id=1730
- Bulletin de sécurité SUSE :
http://www.novell.com/linux/security/advisories/2005_15_openslp.html
- Bulletin de sécurité Mandrake MDKSA-2005:055 du 15 mars 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:055>
- Bulletin de sécurité Gentoo GLSA 200503-25 du 20 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-25.xml>

Gestion détaillée du document

15 mars 2005 version initiale.

17 mars 2005 ajout référence au bulletin de sécurité de Mandrake.

24 mars 2005 ajout référence au bulletin de sécurité de Gentoo.