

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque Libnids

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-2003-AVI-178>

Gestion du document

Référence	CERTA-2003-AVI-178-002
Titre	Vulnérabilité de la bibliothèque Libnids
Date de la première version	03 novembre 2003
Date de la dernière version	06 janvier 2004
Source(s)	–
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.

2 Systèmes affectés

Toutes les applications utilisant une bibliothèque libnids vulnérable. Les versions 1.17 et antérieures de libnids sont vulnérables.

3 Résumé

Une vulnérabilité dans la bibliothèque libnids permet l'exécution de code arbitraire à distance.

4 Description

La bibliothèque libnids offre des fonctionnalités aux systèmes de détection d'intrusions. Elle permet notamment la défragmentation IP et le réassemblage des sessions TCP. Une vulnérabilité dans la fonctionnalité de réassemblage de sessions TCP permet l'exécution de code arbitraire.

5 Solution

Installer la version 1.18 de `libnids` disponible à l'adresse suivante :
<http://prdownloads.sourceforge.net/libnids/>

6 Documentation

- Référence CVE CAN-2003-0850 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0850>
- Site de libnids :
<http://www.packetfactory.net/Projects/libnids/>
- Bulletin de sécurité Gentoo GLSA:200311-07 :
<http://www.securityfocus.com/archive/1/345458/2003-11-22/2003-11-28/0>
- Bulletin de sécurité Debian DSA 410-1 :
<http://www.debian.org/security/2004/dsa-410>

Gestion détaillée du document

03 novembre 2003 version initiale.

25 novembre 2003 ajout du bulletin de sécurité Gentoo.

06 janvier 2004 ajout du bulletin de sécurité Debian.