



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 janvier 2006
N° CERTA-2005-AVI-192-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Net-SNMP

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-192>

Gestion du document

Référence	CERTA-2005-AVI-192-003
Titre	Vulnérabilité de Net-SNMP
Date de la première version	06 juin 2005
Date de la dernière version	27 janvier 2006
Source(s)	Bulletin de sécurité GLSA 200505-18 de Gentoo
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

Atteinte à l'intégrité des données.

2 Systèmes affectés

Net-SNMP version 5.2.1 ou antérieures.

3 Description

Net-SNMP est un ensemble d'outils et bibliothèques liés au protocole SNMP.

Une vulnérabilité liée à la gestion des fichiers temporaires est présente dans l'exécutable `fixproc`. L'exploitation de cette vulnérabilité peut permettre à un utilisateur local de supprimer ou modifier un fichier du système utilisant une version vulnérable de Net-SNMP.

4 Solution

La version 5.1 de `fixproc` présente sur le serveur CVS du projet corrige cette vulnérabilité.
Un correctif est également disponible auprès de certains éditeurs (cf. section Documentation).

5 Documentation

- Site Internet Net-SNMP :
<http://net-snmp.sourceforge.net>
- Bulletin de sécurité Gentoo GLSA 200505-18 du 23 mai 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200505-18.xml>
- Bulletins de sécurité RedHat :
 - Bulletin de sécurité RedHat RHSA-2005:373 du 28 septembre 2005 (v.3) :
<http://rhn.redhat.com/errata/RHSA-2005-373.html>
 - Bulletin de sécurité RedHat RHSA-2005:395 du 05 octobre 2005 (v.4) :
<http://rhn.redhat.com/errata/RHSA-2005-395.html>
- Bulletins de sécurité Linux Fedora :
 - Mise à jour de sécurité pour Fedora Core 3 du 13 juillet 2005 :
<http://www.securityfocus.com/advisories/8880>
 - Mise à jour de sécurité pour Fedora Core 4 du 13 juillet 2005 :
<http://www.securityfocus.com/advisories/8879>
- Bulletin de sécurité OpenBSD pour net-snmp du 25 mai 2005 :
<http://www.vuxml.org/openbsd/pkg-net-snmp.html>
- Bulletin de sécurité FreeBSD pour net-snmp du 09 juillet 2005 :
<http://www.vuxml.org/freebsd/pkg-net-snmp.html>
- Bulletin de sécurité Mandriva MDKSA-2006:025 du 26 janvier 2006 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:025>
- Référence CVE CAN-2005-1740 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1740>

Gestion détaillée du document

06 juin 2005 version initiale.

11 juillet 2005 ajout de la référence CVE CAN-2005-1740 et du bulletin de sécurité FreeBSD.

07 octobre 2005 ajout des bulletins de sécurité RedHat et Fedora.

27 janvier 2006 ajout de la référence au bulletin de sécurité Mandriva.