



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 05 novembre 2008  
N° CERTA-2008-AVI-540-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2008-AVI-540>

---

### Gestion du document

Référence	CERTA-2008-AVI-540-001
Titre	Vulnérabilité dans net-snmp
Date de la première version	05 novembre 2008
Date de la dernière version	20 novembre 2008
Source(s)	Rapport de bogue 2205039 de net-snmp
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.

## 2 Systèmes affectés

- Net-snmp 5.2.x versions antérieures à 5.2.5.1 ;
- net-snmp 5.3.x versions antérieures à 5.3.2.3 ;
- net-snmp 5.4.x versions antérieures à 5.4.2.1.

## 3 Résumé

Une vulnérabilité dans net-snmp permet à une personne malintentionnée d'effectuer un déni de service à distance.

## 4 Description

Une vulnérabilité de type débordement d'entier a été identifiée dans la fonction `netsnmp_create_subtree_cache()` du fichier `agent/snmpd_agent.c` de net-snmp. Son exploitation permet à une personne malintentionnée d'effectuer un déni de service en envoyant une requête GETBULK spécialement conçue à un agent vulnérable.

## 5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Rapport de bogue 2205039 de net-snmp :  
[http://sourceforge.net/tracker/index.php?func=detail&aid=2205039&group\\_id=12694&atid=112694](http://sourceforge.net/tracker/index.php?func=detail&aid=2205039&group_id=12694&atid=112694)
- Bulletin de sécurité RHSA-2008-0971 du 03 novembre 2008 :  
<https://rhn.redhat.com/errata/RHSA-2008-0971.html>
- Bulletin de sécurité Debian DSA-1663 du 09 novembre 2008 :  
<http://www.debian.org/security/2008/dsa-1663>
- Référence CVE CVE-2008-4309 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4309>

## Gestion détaillée du document

**05 novembre 2008** version initiale ;

**20 novembre 2008** ajout de la référence au bulletin Debian DSA-1663 du 09 novembre 2008.