

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de GNATS

---

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-2004-AVI-221>

---

### Gestion du document

Référence	CERTA-2004-AVI-221
Titre	Vulnérabilité de GNATS
Date de la première version	05 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité INetCop #2003-0x82-018
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

Elévation de privilèges.

## 2 Systèmes affectés

- GNATS version 3.002 ;
- GNATS version 3.113 ;
- GNATS version 3.113.1 ;
- GNATS version 3.2.

## 3 Résumé

Plusieurs vulnérabilités dans GNATS permettent à un utilisateur mal intentionné d'élever ses privilèges.

## 4 Description

GNATS est un outil de gestion de rapports de défauts (bug report). Plusieurs débordements de mémoire dans GNATS permettent à un utilisateur mal intentionné d'élever ses privilèges et d'obtenir ceux du super-utilisateur root.

## **5 Contournement provisoire**

Enlever le drapeau `setuid` des binaires GNATS (cela peut entraîner des limitations).

## **6 Solution**

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

## **7 Documentation**

- Site Internet de GNATS :  
<http://www.gnu.org/software/gnats/gnats.html>
- Bulletin de sécurité INetCop :  
<http://x82.inetcop.org/home/adv1sor1es/INCSA.2003-0x82-018-GNATS-bt.txt>
- Bulletin de sécurité FreeBSD pour GNATS du 02 juillet 2004 :  
<http://www.vuxml.org/freebsd/>

## **Gestion détaillée du document**

**05 juillet 2004** version initiale.