

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité de sysstat**

---

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-085>

---

### Gestion du document

Référence	CERTA-2004-AVI-085-001
Titre	Vulnérabilité de sysstat
Date de la première version	15 mars 2004
Date de la dernière version	07 avril 2004
Source(s)	Bulletin de sécurité DSA-460 de Debian Bulletin de sécurité RHSA-2004:053 de Red Hat
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

Corruption de données.

## 2 Systèmes affectés

Versions des sources de `sysstat` antérieures à la version 5.0.2.

## 3 Description

Le paquetage `sysstat` comprend un ensemble d'outils (`sar`, `iostat`, etc.) permettant de visualiser les performances du système.

Une vulnérabilité (mauvaise gestion des fichiers temporaires) présente dans la commande `isag` (outil graphique de visualisation des statistiques) peut être exploitée par un utilisateur mal intentionné afin de corrompre n'importe quel fichier du système accessible en écriture par l'utilisateur lançant la commande `isag`.

## 4 Solution

La version 5.0.2 de `sysstat` corrige cette vulnérabilité.

## 5 Documentation

- Page de sysstat :  
<http://perso.wanadoo.fr/sebastien.godard>
- Bulletin de sécurité DSA-460 de Debian :  
<http://www.debian.org/security/2004/dsa-460>
- Bulletin de sécurité RHSA-2004:093 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-093.html>
- Bulletin de sécurité RHSA-2004:053 de Red Hat :  
<http://rhn.redhat.com/errata/RHSA-2004-053.html>
- Bulletin de sécurité Gentoo GLSA 200404-04 :  
<http://www.gentoo.org/security/en/glsa/glsa-200404-04.xml>
- Référence CVE CAN-2004-0107 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0107>
- Référence CVE CAN-2004-0108 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0108>

### Gestion détaillée du document

**15 mars 2004** version initiale.

**07 avril 2004** ajout du bulletin de sécurité Gentoo et d'une référence CVE.