



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 26 novembre 2001  
N° CERTA-2001-AVI-149

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilités dans le package susehelp de SuSE**

---

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-2001-AVI-149>

---

### Gestion du document

Référence	CERTA-2001-AVI-149
Titre	Vulnérabilités dans le package susehelp de SuSE
Date de la première version	26 novembre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité SuSE
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.

## 2 Systèmes affectés

SuSE 7.2 et 7.3.

## 3 Résumé

Des vulnérabilités dans le package *susehelp* permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine.

## 4 Description

Le package *susehelp* est basé sur un service *http*, et fournit des pages d'aide en ligne aux utilisateurs. Il contient plusieurs scripts CGI qui présentent des vulnérabilités, et permettent ainsi à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine avec les droits du serveur *httpd*.

Par défaut, ce service est démarré, et les droits du serveur sont ceux de l'utilisateur *wwwrun*.

## 5 Contournement provisoire

Arrêter le démon *httpd* ou filtrer l'accès à ce service pour limiter l'exploitation de ces vulnérabilités.

## 6 Solution

Mettre à jour le package *susehelp* suivant la distribution utilisée :

- SuSE-7.3 :  
<ftp://ftp.suse.com/pub/suse/i386/update/7.3/doc1/susehelp-2001.09.06-110.norach.rpm>
- SuSE-7.2 :  
<ftp://ftp.suse.com/pub/suse/i386/update/7.2/doc1/susehelp-2001.05.14-41.noarch.rpm>

## 7 Documentation

Avis de sécurité SuSE 2001:41 :  
<http://www.securityfocus.com/advisories/3675>

## Gestion détaillée du document

26 novembre 2001 version initiale.