

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités sur Webmin

---

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-2002-AVI-105>

---

### Gestion du document

Référence	CERTA-2002-AVI-105
Titre	Vulnérabilités sur Webmin
Date de la première version	17 mai 2002
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq
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 ;
- usurpation d'identité ;
- cross site scripting.

## 2 Systèmes affectés

versions de `webmin` antérieures à la version 0.97.

## 3 Résumé

Plusieurs vulnérabilités présentes dans `webmin` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

webmin est un outil qui permet l'administration de machines à distance via un navigateur Web. webmin est installé par défaut sur certaines distributions.

La première vulnérabilité de type « cross site scripting » présente dans la gestion des messages d'erreurs permet à un utilisateur mal intentionné de faire exécuter du code sur la machine de l'utilisateur visualisant ces messages d'erreurs.

Une seconde vulnérabilité présente dans la gestion de l'authentification permet à un utilisateur mal intentionné de contourner l'authentification par mot de passe.

## 5 Contournement provisoire

Filter le port 10000/tcp au niveau du garde-barrière.

## 6 Solution

Mettre à jour webmin avec la version 0.97 (se référer à la section documentation).

## 7 Documentation

- Site de webmin :  
<http://www.webmin.com>
- Avis de sécurité 4694 de SecurityFocus :  
<http://online.securityfocus.com/bid/4694>
- Avis de sécurité 4700 de SecurityFocus :  
<http://online.securityfocus.com/bid/4700>

## Gestion détaillée du document

17 mai 2002 version initiale.