

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-061>

Gestion du document

Référence	CERTA-2002-AVI-061
Titre	Vulnérabilité sur webmin
Date de la première version	25 mars 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

Elévation de privilèges en local.

2 Systèmes affectés

webmin version 0.92-1.

3 Résumé

Un utilisateur mal intentionné peut, en utilisant des informations présentes dans un fichier journal, se connecter à la machine avec les privilèges du super utilisateur (`root`).

4 Description

webmin est une interface web qui permet l'administration d'un système en local ou à distance depuis n'importe quel navigateur supportant les formulaires et les tableaux.

Des permissions accordées par défaut sur le répertoire `/var/webmin/` lors de l'installation de `webmin` permettent à un utilisateur mal intentionné de récupérer l'identifiant (`sid`) du super utilisateur (`root`) dans le fichier journal `webmin.log`. Cette information peut ensuite être réutilisée pour se connecter en tant que super utilisateur.

Cette vulnérabilité est exploitable en local.

5 Contournement provisoire

Supprimer les permissions de lecture et d'écriture du répertoire `/var/webmin/` pour les utilisateurs autres que le super utilisateur.

6 Solution

Mettre à jour la dernière version de `webmin`.

7 Documentation

Site officiel de `webmin`
<http://www.webmin.com>

Gestion détaillée du document

25 mars 2002 version initiale.