

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Webmin et Usermin

---

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-2005-AVI-356>

---

### Gestion du document

Référence	CERTA-2005-AVI-356-001
Titre	Vulnérabilité de Webmin et Usermin
Date de la première version	20 septembre 2005
Date de la dernière version	26 septembre 2005
Source(s)	Liste des changements dans Webmin/Usermin du 20 septembre 2005
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- Webmin versions 1.220 et antérieures ;
- Usermin versions 1.150 et antérieures.

## 3 Résumé

Une vulnérabilité dans Webmin et Usermin permet à un utilisateur distant de contourner la politique de sécurité du système vulnérable.

## 4 Description

Webmin et Usermin permettent l'administration à distance de machine via une interface web. Une erreur dans la mise en œuvre de l'authentification des utilisateurs dans ces deux logiciels permet à un utilisateur distant mal intentionné d'accéder à Webmin ou Usermin sans s'authentifier préalablement.

Remarque : la vulnérabilité n'est exploitable que si l'option "full PAM conversations" a été activée dans l'interface de configuration de l'authentification. Ce n'est pas le cas par défaut.

## 5 Solution

Mettre à jour :

- Webmin en version 1.230 disponible à l'adresse :  
<http://www.webmin.com/download.html>
- Usermin en version 1.160 disponible à l'adresse :  
<http://www.webmin.com/udownload.html>

## 6 Documentation

- Site Internet de Webmin et Usermin :  
<http://www.webmin.com>
- Liste des changements dans Webmin :  
<http://www.webmin.com/changes-1.230.html>
- Liste des changements dans Usermin :  
<http://www.webmin.com/uchanges-1.160.html>
- Bulletin de sécurité SNS No. 83 du 20 septembre 2005 :  
[http://www.lac.co.jp/business/sns/intelligence/SNSadvisory\\_e/83\\_e.html](http://www.lac.co.jp/business/sns/intelligence/SNSadvisory_e/83_e.html)
- Bulletin de sécurité Gentoo GLSA 200509-17 du 24 septembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200509-17.xml>
- Référence CVE CAN-2005-3042 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3042>

## Gestion détaillée du document

**20 septembre 2005** version initiale.

**26 septembre 2005** ajout du lien vers les changements Usermin ainsi que des références aux bulletins de sécurité SNS No. 83, Gentoo GLSA 200509-17 et CVE CAN-2005-3042.