

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Linux PAM

---

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-2010-AVI-530>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2010-AVI-530                          |
| Titre                       | Multiples vulnérabilités dans Linux PAM     |
| Date de la première version | 03 novembre 2010                            |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de sécurité PAM du 28 octobre 2010 |
| 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 ;
- élévation de privilèges.

## 2 Systèmes affectés

Linux PAM versions antérieures à 1.1.3.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans Linux PAM. Elles permettent à un utilisateur malveillant d'élever ses privilèges et de dévoiler des informations sensibles.

## 4 Description

Les vulnérabilités découvertes dans Linux PAM sont les suivantes :

- une erreur dans le module *pam\_mail* permet de vérifier la présence de certains courriels ;

- une erreur dans le module *pam\_env* permet à un utilisateur malveillant d’afficher un fichier arbitraire situé sur le système ;
- une erreur dans le module *pam\_namespace* permet à un utilisateur malveillant d’élèver ses privilèges.

## 5 Solution

Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité PAM du 28 octobre 2010 :  
[http://pam.cvs.sourceforge.net/viewvc/pam/Linux-PAM/ChangeLog?revision=1.546&view=markup&pathrev=Linux-PAM-1\\_1\\_3](http://pam.cvs.sourceforge.net/viewvc/pam/Linux-PAM/ChangeLog?revision=1.546&view=markup&pathrev=Linux-PAM-1_1_3)
- Référence CVE CVE-2010-3430 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3430>
- Référence CVE CVE-2010-3431 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3431>
- Référence CVE CVE-2010-3435 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3435>
- Référence CVE CVE-2010-3853 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3853>

## Gestion détaillée du document

03 novembre 2010 version initiale.