

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans libpango

---

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-2011-AVI-129>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2011-AVI-129   |
| Titre                       | Vulnérabilités dans libpango   |
| Date de la première version | 03 mars 2011   |
| Date de la dernière version | –  |
| Source(s)                   | Rapport de bug Gnome n639882 du 18 janvier 2011<br>Rapport de bug Ubuntu n696616 du 02 mars 2011 |
| 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 à distance ;
- déni de service à distance.

## 2 Systèmes affectés

Libpango versions 1.28.3 et précédentes.

## 3 Résumé

Deux vulnérabilités ont été corrigées dans la bibliothèque libpango. Elles peuvent être exploitées pour réaliser un déni de service à distance, et dans certains cas exécuter du code à distance.

## 4 Description

Deux vulnérabilités affectent libpango. La première (CVE-2011-0020) permet à un attaquant de réaliser un déni de service en provoquant l'arrêt brutal d'une application utilisant cette bibliothèque à l'aide d'un fichier de police

de caractères spécialement conçu. Le débordement de tampon sur le tas est à l'origine de l'arrêt, et pourrait être exploité pour exécuter du code à distance. La seconde (CVE-2011-0064) permet à une personne malveillante de provoquer l'arrêt brutal d'une application via un déréférencement de pointeur NULL, en lui passant des paramètres spécialement conçus. L'exécution de code arbitraire à distance est également possible.

## 5 Solution

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

## 6 Documentation

- Rapport de bug Gnome n639882 du 18 janvier 2011 :  
[http://bugzilla.gnome.org/show\\_bug.cgi?id=639882](http://bugzilla.gnome.org/show_bug.cgi?id=639882)
- Rapport de bug Debian n610792 du 24 janvier 2011 :  
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=610792>
- Bulletin de sécurité RedHat RHSA-2011:0180 du 27 janvier 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-0180.html>
- Bulletin de sécurité Ubuntu USN-1082-1 du 02 mars 2011 :  
<http://www.ubuntu.com/usn/usn-1082-1>
- Bulletin de sécurité Debian DSA 2178 du 02 mars 2011 :  
<http://www.debian.org/security/2011/dsa-2178>
- Bulletin de sécurité RedHat RHSA-2011:0309 du 03 mars 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-0309.html>
- Référence CVE CVE-2011-0020 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0020>
- Référence CVE CVE-2011-0064 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0064>

## Gestion détaillée du document

**03 mars 2011** version initiale.