

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans evince

---

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-005>

---

### Gestion du document

Référence	CERTA-2011-AVI-005-001
Titre	Multiples vulnérabilités dans evince
Date de la première version	07 janvier 2011
Date de la dernière version	11 janvier 2011
Source(s)	Bulletin de sécurité Ubuntu USN-1035-1 du 05 janvier 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.

## 2 Systèmes affectés

evince versions 2.x.

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans *evince*, un lecteur de documents pouvant lire différents formats de fichiers (PDF, DVI, PostScript) pour l'environnement de bureau *GNOME*. L'exploitation réussie de celles-ci peut permettre l'exécution de code arbitraire à distance.

## 4 Description

Quatre vulnérabilités dans le moteur de rendu de fichiers DVI ont été corrigées. En forçant un utilisateur à afficher un fichier DVI spécialement conçu, un attaquant peut terminer l'exécution d'*evince* ou exécuter du code arbitraire avec les droits de cet utilisateur.

## 5 Solution

Se référer aux bulletins de sécurité des différentes distributions utilisant ce logiciel pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Système de gestion de code source du projet evince :  
<http://git.gnome.org/browse/evince/commit/?id=d4139205b010ed06310d14284e63114e88ec6de2>
- Bulletin de sécurité Red Hat :  
<https://rhn.redhat.com/errata/RHSA-2011-0009.html>
- Bulletin de sécurité Ubuntu USN-1035-1 du 05 janvier 2011 :  
<http://www.ubuntu.com/usn/usn-1035-1>
- Bulletin de sécurité Fedora FEDORA-2011-0208 du 07 janvier 2011 :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-January/052910.html>
- Référence CVE CVE-2010-2640 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2640>
- Référence CVE CVE-2010-2641 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2641>
- Référence CVE CVE-2010-2642 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2642>
- Référence CVE CVE-2010-2643 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2643>

## Gestion détaillée du document

**07 janvier 2011** version initiale ;

**11 janvier 2001** ajout du correctif Fedora.