

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Ghostscript

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-2008-AVI-113>

Gestion du document

Référence	CERTA-2008-AVI-113-001
Titre	Vulnérabilité de Ghostscript
Date de la première version	03 mars 2008
Date de la dernière version	03 mars 2008
Source(s)	CVE-2008-0411
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

Ghostscript, versions 8.x.

3 Résumé

Une vulnérabilité dans *Ghostscript* permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Ghostscript permet la visualisation de documents au format Postscript.

La fonction `zseticcspace()` ne vérifie pas la longueur d'un tableau. Cette vulnérabilité permet de provoquer un débordement de pile. L'exploitation de cette vulnérabilité permet à un utilisateur malveillant d'exécuter du code arbitraire à distance par le biais d'un document Postscript conçu à cet effet.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1510 du 27 février 2008 :
<http://www.debian.org/security/2008/dsa-1510>
- Bulletin de sécurité Fedora du 03 mars 2008 :
<http://www.redhat.com/archives/fedora-package-announce/2008-March/msg00085.html>
- Bulletin de sécurité Mandriva MDVSA-2008:055 du 29 février 2008 :
<http://www.mandriva.com/archives/security/advisories?name=MDVSA-2008:055>
- Bulletin de sécurité RedHat RHSA-2008:0155 du 27 février 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0155.html>
- Bulletin de sécurité Suse SUSE-SA:2008:010 du 28 février 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00009.html>
- Référence CVE CVE-2008-0411 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0411>

Gestion détaillée du document

03 mars 2008 version initiale.

06 mars 2008 ajout de la référence Fedora.