

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de scrollkeeper

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-2002-AVI-200>

Gestion du document

Référence	CERTA-2002-AVI-200
Titre	Vulnérabilité de scrollkeeper
Date de la première version	04 septembre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité RHSA-2002:186 de Red Hat
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

- Corruption de fichiers ;
- déni de service.

2 Systèmes affectés

Scrollkeeper versions 3.0 à 3.11.

3 Résumé

En exploitant une vulnérabilité présente dans l'application scrollkeeper, un utilisateur local peut corrompre n'importe quel fichier du système.

4 Description

Scrollkeeper est une application permettant de gérer la documentation d'un système. Scrollkeeper est utilisée depuis des applications telles le navigateur `khelpcenter` (aide en ligne sous KDE) ou `nautilus` (gestionnaire de fichiers sous GNOME 1.4).

L'exécutable `/usr/bin/scrollkeeper-get-cl` crée des fichiers temporaires avec des noms prédictibles. Sous certaines conditions, un utilisateur mal intentionné peut exploiter cette vulnérabilité pour corrompre n'importe quel fichier du système. Cette vulnérabilité ne peut être exploitée que par un utilisateur possédant un compte local.

5 Solution

Des mises à jour sont disponibles sous forme de paquetages pour les distributions Linux (cf. section Documentation).

6 Documentation

- Projet scrollkeeper :
<http://sourceforge.net/projects/scrollkeeper>
- Bulletin de sécurité RHSA-2002:186 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2002-166.html>
- Bulletin de sécurité DSA-160 de Debian :
<http://www.debian.org/security/2002/dsa-160>

Gestion détaillée du document

04 septembre 2002 version initiale.