

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du paquetage util-linux

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-159>

Gestion du document

Référence	CERTA-2002-AVI-159
Titre	Vulnérabilité du paquetage util-linux
Date de la première version	30 juillet 2002
Date de la dernière version	–
Source(s)	Avis de sécurité "Linux util-linux chfn local root vulnerability" de Razor
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

Elévation de privilèges.

2 Systèmes affectés

Red Hat Linux version 7.3 et versions antérieures.

3 Résumé

Une vulnérabilité de type problème d'accès concurrent ("race condition") permet à un utilisateur mal intentionné d'obtenir les privilèges de l'administrateur système.

4 Description

La commande `chfn` ainsi que `chsh` permettent de modifier le fichier `/etc/passwd`. Ces binaires sont fournis dans le paquetage `util-linux`.

Sous certaines conditions, un utilisateur mal intentionné peut exploiter une vulnérabilité de type gestion des accès concurrents pour modifier le fichier `/etc/passwd` et créer une nouvelle entrée correspondant à un compte privilégié.

Cette vulnérabilité n'est exploitable que par un utilisateur ayant un compte local à la machine.

5 Contournement provisoire

Il est possible d'empêcher l'exploitation de cette vulnérabilité en retirant le drapeau `setuid root` des binaires `/usr/bin/chfn` et `/usr/bin/chsh` au moyen de la commande `chmod u-s`.

6 Solution

Consulter le bulletin de sécurité correspondant à la distribution Linux utilisée (Cf. section documentation ci-dessous).

7 Documentation

Avis de sécurité RHSA-2002:132 de RedHat :
<http://rhn.redhat.com/errata/RHSA-2002-132.html>

Gestion détaillée du document

30 juillet 2002 version initiale.