

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans rsync

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-2007-AVI-371>

Gestion du document

Référence	CERTA-2007-AVI-371
Titre	Vulnérabilités dans rsync
Date de la première version	22 août 2007
Date de la dernière version	–
Source(s)	Annonce de sécurité Mandriva MDKSA-2007:166 du 18 août 2007
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- rsync version 2.6.9 ainsi que les versions antérieures.

3 Résumé

Des vulnérabilités ont été identifiées dans l'utilitaire rsync. L'exploitation de ces dernières permettrait à une personne malveillante de perturber le système, voire d'élever ses privilèges ou exécuter du code arbitraire.

4 Description

Des vulnérabilités ont été identifiées dans l'utilitaire rsync. Parmi celles-ci, il y aurait un mauvais décalage d'indice (*off-by-one*) dans la fonction `f_name()` qui permettrait à une personne de contourner la politique de sécurité en trichant sur les noms de répertoires.

5 Solution

Se référer aux différents bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Page du projet rsync :
<http://samba.anu.edu.au/rsync/>
- Bulletin de sécurité Mandriva MDKSA-2007:166 du 18 août 2007 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:166>
- Communiqué de RedHat sur le bogue du 15 août 2007 :
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=CVE-2007-4091#c1
- Bulletin de sécurité SUSE SuSE-SA:2007:017 du 17 août 2007 :
http://www.novell.com/linux/security/advisories/2007_17_sr.html
- Bulletin de sécurité Ubuntu USN-500-1 du 20 août 2007 :
<http://www.ubuntulinux.org/usn/usn-500-1>
- Référence CVE CVE-2007-4091 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2007-4091>

Gestion détaillée du document

22 août 2007 version initiale.